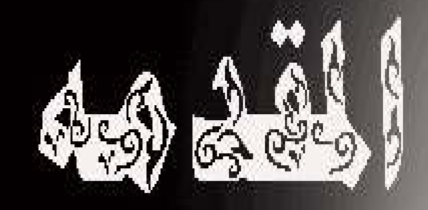

الحمايه تحت المجهر
اعداد: القرصان
مراجعة الشروحات
MR,X
مراجعه املائيه وتحقيق
اميره
HACKER
SECURITY FROM



الحمد لله رب العالمين والصلاة والسلام على سيدنا محمد وعلى آله وصحبه أجمعين.. وبعد:

فأن الهكر كلمه اطلقت على المبرمجين المهره القادرين على التعامل مع الكمبيوتر بخبره

ودرايه حيث انهم كانو يقدمون الحلول البرمجيه بشكل طوعي ((غالباً))

ولكن في بداية 1980م بدأ ((الكركرز)) وهم مجموعه من المخربين ولصوص البرامج

المصممه من قبل الهكرز ليستغلوها في تنفيذ اختراقاتهم ويستخدمونها بعشوائيه

ويتسببون بدمار واسع لأجهزة الحاسوب مما اضطر الهكر والمبرمجون المحترفون الى تصميم

برامج الحمايه لصدهم او لتجنب الظرر الناتج من اختراقاتهم

ويسرنا في هذا الكتاب ((الحمايه تحت المجهر)) شرح اهم اساليب وطرق ممالقة الهكر في حماية

الاجهزه

كما اننا ننوه بانه لا يمكن حماية اي جهاز 100٪ ولكن سنجتهد في هذا الكتاب لطرح افضل

الطرق واسهلها

هذا والله ولي التوفيق .

القرصان 2008

الفصل الاول

((الفايروسات))

عندما تحدثت التقارير في عام 1989 عن أول فيروسات الكمبيوتر ، خيل للكثيرين (ومن بينهم خبراء في هذا المجال (أن ذلك مجرد خرافة ابتدعها أحد كتاب قصص الخيال العلمي ، وأن وسائل الإعلام تحاول أن ترسخها في أذهان الناس كحقيقة رغم أنها لا تمت إلى الواقع بصلة . لقد امتدت تلك الظاهرة واتسعت حتى باتت تشكل خطراً حقيقياً يهدد الثورة المعلوماتية التي فجرتها التقنيات المتطورة والمتسارعة في علوم الكمبيوتر. فمن بضعة فيروسات لا تزيد عن عدد أصابع اليد في السنة الأولى إلى ما يزيد عن (5000 1) فيروس في يومنا هذا ، وفي كل يوم تكتشف أنواع جديدة من الفيروسات المختلفة التأثير مما يقلق مستخدم الكمبيوتر ويسلبهم راحة البال . ومن فيروسات بسيطة الضرر والتأثير يسهل اكتشافها والتخلص منها مروراً بفيروسات خبيثة بالغة الأذى تجيد التخفي ويطول زمن اكتشافها إلى فيروسات ماكرة ذكية تبرع في التغير والتحول من شكل لآخر مما يجعل تقفي أثرها وإلغاء ضررها أمرا صعبا. أما الأسباب التي تدفع بعض الناس لكتابة البرامج الفيروسية فمنها :

1الحد من نسخ البرامج كما في فيروس brain أوPakistani وهو أول فيروسات الكمبيوتر ظهورا وأكثرها انتشارا وكتب من قبل أخوين من الباكستان كحماية للملكية الفكرية للبرامج التي قاما بكتابتها .

-2البحث العلمي كما في فيروس.STONED الشهير والذي كتبه طالب دراسات عليا في نيوزيلندة وسرق من قبل أخيه الذي أراد أن يداعب أصدقاءه بنقل الفيروس إليهم .

-3الرغبة في التحدي وإبراز المقدرة الفكرية من بعض الأشخاص الذين يسخرون ذكاءهم وقدراتهم بشكل سيئ ، مثل فيروسات V2P التي كتبها Mark Washburn كإثبات أن البرامج المضادة للفيروسات من نوع Scanners غير فعالة .

-4الرغبة في الانتقام من قبل بعض المبرمجين المطرودين من أعمالهم والناقمين على شركاتهم وتصمم الفيروسات في هذه الحالة بحيث تنشط بعد تركهم العمل بفترة كافية أي تتضمن قنبلة منطقية موقوتة .

-5التشجيع على شراء البرامج المضادة للفيروسات إذ تقوم بعض شركات البرمجة بنشر فيروسات جديدة ثم تعلن عن منتج جديد لكشفهما .

يعرف الفيروس في علم الأحياء على أنه جزيئة صغيرة من مادة حية غير قادرة على التكاثر ذاتياً ولكنها تمتلك مادة وراثية كافية لتمكينهما من الدخول إلى خلية حية وتغيير العمليات الفعالة في الخلية بحيث تقوم تلك الخلية بإنتاج جزيئات جديدة من ذلك الفيروس و التي تستطيع بدورها مهاجمة خلايا جديدة.

و بشكل مشابه ، يعرف الفيروس في علم الكمبيوتر على أنه برنامج صغير أو جزء من برنامج يربط نفسه ببرنامج آخر ولكنه يغير عمل ذلك البرنامج لكي يتمكن الفيروس من التكاثر عن طريقه.

ويتصف فيروس الكمبيوتر بأنه : برنامج قادر على التناسخ Replication والانتشار أي خلق نسخ (قد تكون معدلة) من نفسه . وهذا ما يميز الفيروس عن البرامج الضارة الأخرى التي لا تكرر نفسها مثل أحصنة طروادة Trojans والقنابل المنطقية. Bombs عملية التناسخ ذاتها هي عملية مقصودة وليست تأثيراً جانبيا وتسبب خللاً أو تخريباً في نظام الكمبيوتر المصاب إما بشكل عفوي أو متعمد ويجب على الفيروس أن يربط نفسه ببرنامج

أخر يسمى البرنامج الحاضن HOST بحيث أن أي تنفيذ لذلك البرنامج سيضمن تنفيذ الفيروس، هذا ما يميز الفيروس عن الديدان worms التي لا تحتاج إلى ذلك.

(آلية عمل الفيروس و أنواعه)

آلية عمل الفيروسات:

للفيروس أربعة آليات أثناء انتشاره في الكمبيوتر الضحية:

1-آلية التناسخ Replication

وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه و بدونه لا يمكن للبرنامج أن يكرر ذاته وبالتالي فهو ليس فيروساً.

2-آلية التخفيThe Protection Mechanism

وهو الجزء الذي يخفي الفيروس عن الاكتشاف ويمكن أن يتضمن تشفير الفيروس لمنع البرامج الماسحة التي تبحث عن نموذج الفيروس من اكتشافه.

3-آلية التنشيط Activate

وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة كما في فيروس MICHELANGELOالذي ينشط في السادس من آذار من كل عام وهنالك فيروسات تنتظر حتى تنفذ برنامج ما عددا معين من المرات كما في فيروس ICELAND ،و كما في فيروس TAIWAN الذي يسبب تهيئة القرص الصلب بعد (90) إقلاع للكمبيوتر ،وفيروس MANCHU الذي ينشط عند الضغط على مفاتيح CTRL+ALT+DEL .

تعمل الفيروسات بطرق مختلفة، وسنعرض فيما يلي للطريقة العامة التي تنتهجها كافة الفيروسات. في البداية يظهر الفيروس على جهازك، ويكون قد دخل إليه مختبئاً في ملف برنامج ملوث (مثل ملفات COM أو EXEأو قطاع الإقلاع). وكانت الفيروسات في الماضي تنتشر بشكل أساسي عن طريق توزيع أقراص مرنة ملوثة. أما اليوم، فمعظمها يأتي مع البرامج المنقولة عبر الشبكات (ومن بينها إنترنت)، كجزء من برنامج تركيب نسخة تجريبية من تطبيق معين، أو ماكرو لأحد التطبيقات الشهيرة، أو كملف مرفق (attachment)برسالة بريد إلكتروني.
ويجدر التنويه إلى أن رسالة البريد الإلكتروني نفسها لا يمكن أن تكون فيروساً، فالفيروس برنامج، ويجب تشغيله لكي يصبح نشطاً. إذاً الفيروس المرفق برسالة بريد إلكتروني، لا حول له ولا قوة، إلى أن تشغّله.
ويتم تشغيل فيروسات المرفقات عادة، بالنقر عليها نقرة مزدوجة بالماوس .ويمكنك حماية جهازك من هذه الفيروسات، بالامتناع عن تشغيل أي ملف مرفق برسالة بريد إلكتروني، إذا كان امتداده COM أوEXE ، أو إذا كان أحد ملفات بيانات التطبيقات التي تدعم الماكرو، مثل برامج أوفيس، إلى ما بعد فحصه والتأكد من خلوه من الفيروسات. أما ملفات الرسوميات والصوت ، وأنواع ملفات البيانات الأخرى القادمة كمرفقات، فهي آمنة، ولا يمكن للفيروس أن ينشط من خلالها، ولذلك فهو لا يهاجمها.

إذاً يبدأ الفيروس دورة حياته على الجهاز بشكل مشابه لبرنامج حصان طروادة، فهو يختبئ في ثنايا برنامج أو ملف آخر، وينشط معه. في الملفات التنفيذية الملوثة، يكون الفيروس قد أضاف شيفرته إلى البرنامج الأصلي، وعدل تعليماته بحيث ينتقل التنفيذ إلى شيفرة الفيروس .وعند تشغيل الملف التنفيذي المصاب، يقفز البرنامج عادة إلى تعليمات الفيروس، فينفذها، ثم يعود ثانية لتنفيذ تعليمات البرنامج الأصلي. وعند هذه النقطة يكون الفيروس نشطاً، وجهازك أصبح ملوثاً ،وقد ينفذ الفيروس مهمته فور تنشيطه ويطلق عليه فيروس العمل المباشر direct-action أو يقبع منتظراً في الذاكرة، باستخدام وظيفة " الإنهاء والبقاء في الذاكرة terminate and stay resident, TSR التي تؤمنها نظم التشغيل عادة .

وتنتمي غالبية الفيروسات لهذه الفئة، ويطلق عليها الفيروسات" المقيمة". ونظراً للإمكانيات الكبيرة المتاحة

للبرامج المقيمة في الذاكرة، بدءاً من تشغيل التطبيقات والنسخ الاحتياطي للملفات إلى مراقبة ضغطات لوحة المفاتيح ونقرات الماوس (والكثير من الأعمال الأخرى)، فيمكن برمجة الفيروس المقيم، لتنفيذ أي عمل يمكن أن يقوم به نظام التشغيل، تقريباً . يمكن تشغيل الفيروس المقيم كقنبلة، فيبدأ مهمته على جهازك عند حدث معين. ومن الأمور التي تستطيع الفيروسات المقيمة عملها، مسح (scan) قرصك الصلب وأقراص الشبكة بحثاً عن الملفات التنفيذية، ثم نسخ نفسها إلى هذه الملفات وتلويثها .

أنواع الفيروسات:

يبحث مطورو الفيروسات، بشكل دائم، عن طرق جديدة لتلويث كمبيوترك ، لكن أنواع الفيروسات معدودة عملياً، وتصنف إلى: فيروسات قطاع الإقلاع(boot sector viruses) ، وملوثات الملفات (file infectors)، وفيروسات الماكرو (macro viruses) ، وتوجد أسماء أخرى لهذه الفئات، وبعض الفئات المتفرعة عنها، لكن مفهومها يبقى واحداً.
تقبع فيروسات قطاع الإقلاع في أماكن معينة على القرص الصلب ضمن جهازك، وهي الأماكن التي يقرأها الكمبيوتر وينفذ التعليمات المخزنة ضمنها، عند الإقلاع. تصيب فيروسات قطاع الإقلاع الحقيقية منطقة قطاع الإقلاع الخاصة بنظام دوس(DOS boot record) ، بينما تصيب فيروسات الفئة الفرعية المسماة MBR viruses، قطاع الإقلاع الرئيسي للكمبيوتر .(master boot record) يقرأ الكمبيوتر كلا المنطقتين السابقتين من القرص الصلب عند الإقلاع ، مما يؤدي إلى تحميل الفيروس في الذاكرة. يمكن للفيروسات أن تصيب قطاع الإقلاع على الأقراص المرنة، لكن الأقراص المرنة النظيفة، والمحمية من الكتابة، تبقى أكثر الطرق أمناً لإقلاع النظام، في حالات الطوارئ. والمشكلة التي يواجهها المستخدم بالطبع، هي كيفية التأكد من نظافة القرص المرن، أي خلوه من الفيروسات، قبل استخدامه في الإقلاع، وهذا ما تحاول أن تفعله برامج مكافحة الفيروسات.

تلصق ملوثات الملفات (وتدعى أيضاً الفيروسات الطفيلية (parasitic viruses نفسها بالملفات التنفيذية، وهي أكثر أنواع الفيروسات شيوعاً. وعندما يعمل أحد البرامج الملوثة، فإن هذا الفيروس، عادة، ينتظر في الذاكرة إلى أن يشغّل المستخدم برنامجاً آخر، فيسرع عندها إلى تلويثه. وهكذا، يعيد هذا النوع من الفيروس إنتاج نفسه، ببساطة، من خلال استخدام الكمبيوتر بفعالية، أي بتشغيل البرامج! وتوجد أنواع مختلفة من ملوثات الملفات، لكن مبدأ عملها واحد.

تعتمد فيروسات الماكرو(macro viruses) ، وهي من الأنواع الحديثة نسبياً، على حقيقة أن الكثير من التطبيقات تتضمن لغات برمجة مبيتة ضمنها. وقد صممت لغات البرمجة هذه لمساعدة المستخدم على أتمتة العمليات المتكررة التي يجريها ضمن التطبيق، من خلال السماح له بإنشاء برامج صغيرة تدعى برامج الماكرو. تتضمن برامج طاقم أوفيس، مثلاً، لغة برمجة مبيتة، بالإضافة إلى العديد من برامج الماكرو المبيتة أيضاً، والجاهزة للاستخدام المباشر. وفيروس الماكرو ببساطة، هو برنامج ماكرو مصمم للعمل مع تطبيق معين، أو عدة تطبيقات تشترك بلغة برمجة واحدة. أصبحت فيروسات الماكرو شهيرة بفضل الفيروس المصمم لبرنامج مايكروسوفت وورد. فعندما تفتح وثيقة أو قالباً ملوثين، ينشط الفيروس ويؤدي مهمته التخريبية. وقد بُرمِج هذا الفيروس لينسخ نفسه إلى ملفات الوثائق الأخرى، مما يؤدي إلى ازدياد انتشاره مع استمرار استخدام البرنامج.

ويجمع نوع رابع يدعى الفيروس "متعدد الأجزاء (multipartite) "بين تلويث قطاع الإقلاع مع تلويث الملفات، في وقت واحد.

ستجد قائمة ضخمة بأسماء الفيروسات، مع شرح تفصيلي عن آثار كل منها، في قسم Virus Encyclopediaمن موقع مختبر مكافحة الفيروسات، الخاص بشركةSymantic ، التي تنتج برنامج نورتون أنتي فايروس الشهير

نماذج من الفيروسات

هناك عدة برامج مصممة خصيصا للعمل في بيئة الإنترنت بحيث يتم ارسال هذه البرامج عبر الشبكة بكل سهولة و يسر و يتم تحميلها على جهازك و كأنها معلومات مرسلة إليك دون أي مشاكل أو صعوبات كما أن هذه البرامج قد صممت في الأساس لكي توفر السهولة و السرعة أثناء التصفح أو الإبحار في الشبكة و تجعل من صفحات المواقع أكثر جاذبية و حركة و لذلك تحمست الشركات المنتجة للمتصفحات و قدمت الدعم لهذه التكنولوجيا و لكن للأسف صاحب هذا الانتشار نوع من سوء الاستخدام من قبل بعض المبرمجين و المستخدمين مما تسبب في الكثير من المشاكل الأمنية لبقية المستخدمين ، فتعالوا معنا اليوم لنتعرف سويا على هذه البرامج الخطيرة و طرق الوقاية من مشاكلها

أنواع البرامج ذاتية التحميل.

برامج أكتف إكس. (ActiveX)
برامج جافا أبليتس. (Java Applets)
برامج جافا سكريبت. (Java Scripts)

برامج أكتف إكس. (ActiveX)
هذا البرنامج أحد منتجات شركة مايكروسوفت وهي عبارة عن مجموعة من المتحكمات المبرمجة بواسطة برنامج مايكروسوفت فيجوال بيسك وهي صممت أساساً لتوجيه بعض التقنيات المستخدمة لإنشاء الصفحات المتطورة جداً مثل:

- Component Object Model COM
- Object Linking and Embedding Function OLE

هذه المتحكمات تمكن مصممي الصفحات من إنشاء صفحات بها الكثير من الحركات و الخصائص الجذابة

و مصدر الخطر هي أن هذه المتحكمات إذا ما نزلت إلى جهازك فلا يوجد حدود أو قيود لتقف عندها فهي تستطيع أن تقوم بالمهمات التالية:

-التحكم بنظام التشغيل في جهازك و ذلك بحذف أو تعديل الملفات.
-التحكم في قرصك الصلب و هذا يجعل من مهمة إنزال برامج التجسس و الفيروسات أمر سهل

ارسال معلومات عن نظام التشغيل لديك و بقية . المكونات إلى جهاز آخر أو جهاز خادم بعيد عنك دون معرفتك.
-نقل الملفات من الجهاز إلى أي جهاز آخر مما يسهل من عملية جمع المعلومات الشخصية و كلمات العبور
القدرة على تعديل مستوى الأمن في متصفحك دون علمك وبالتالي تسهيل المهمة لأي برنامج تجسس آخر
برامج جافا أبليتس. (Java Applets)
هي برامج صغيرة و شبيهه جدا بالأكتف اكس لدرجة أننا قد نستطيع القول بأنها نسخة شركة صن مايكروسيستمز و لها نفس مقدرات الأكتف اكس و خطورتها على أمن وخصوصية المستخدم.

برامج جافا سكريبت. (Java Scripts)
هو برنامج مختلف عن الجافا أبليتس و لكنه مشابه له بالإسم و هي عبارة عن مجموعة من المتفرعات للغة الترميز . HTML

أين مصدر الخطر و التهديد ؟

هذا البرنامج قادر على فتح و إغلاق النوافذ أثناء عملك على الشبكة و لذلك تستخدم بكثرة في برامج المحادثات المباشرة و تكمن خطورته في قدرته على تعديل خصائص المتصفح لديك و السماح بإنزال و تشغيل الجافا أبليتس دون علمك و بالتالي التمكن من قراءة القرص الصلب و نقل المعلومات من جهازك كما تتمكن هذه البرامج من التحكم بالاستمارات و الاستبيانات التي تقوم بتعبئتها

أحصنة طروادة. (Trojans)

هي أحد البرامج التي تبدو آمنه و مفيدة و لكنها في الحقيقة تقوم بأعمال غير مشروعة في الخفاء وذلك نتيجة لزرع أحد البرامج الذاتية التشغيل بها دون علمك ، و هناك عدة طرق و حيل يستخدمها الهاكرز لتنزيل أحصنه طروادة في أجهزة الغير بدون علمهم و منها الرسائل الإلكترونية و البطاقات الإلكترونية أو البرامج المجانية مجهولة المصدر و المواقع الشخصية و كثيرة هي المواقع الشخصية العربية التي ما أن تدخل عليها الا و تجد أن هناك برنامج يتم تحميله مباشرة و في الغالب ما يكون برنامج للتحكم بالفأرة وتغيير شكل الفأرة و أنت قد تظن بأن هذا البرنامج مفيد و غير ضار ولكن في الحقيقة هو حصان طروادة و كذلك قد يتم اغراؤك بتنزيل لعبة أو بطاقة الكترونية جميلة أو ملف ملحق برسالة الكترونية وهو في الغالب حصان طروادة.
الوقاية من أحصنة طروادة
دائماً و أبداً الوقاية خير من العلاج و لذلك قم بإتباع النصائح التالية:
-استخدام برنامج مضاد للفيروسات حديث و قم بتجديد الملفات كل فترة من الزمن اقتناء و استخدام جدران النارية.
-عدم تحميل أي برنامج مجاني مجهول المصدر و خاصة إذا كان من موقع شخصي أو من موقع مشبوه.
-تجنب فتح الرسائل الإلكترونية ذات المصادر الغير معروفة خاصة تلك التي تحمل ملفات مرفقة.

-تعديل مستوى الأمن في المتصفح بحيث لا يتم قبول نزول أي برنامج من هذه البرامج.
-اذا لم ترغب في منع هذه البرامج بشكل تام فيمكنك قبول البرامج التي تحمل التوقيع الإلكتروني لمصدرها

((طرق التخلص من اخطر الفايروسات))

ازالة فايروس يوماها

طريقة التخلص من الفيروس

اذا نزل الفيروس وشغلته اول شي تعمله هوه تحديث النورتن انتي فايروس
اعادة تشغيل الجهاز
نسخ ملف
Copy Regedit.exe
الى
Reg.com
وذلك حسب الخطوات التالية وحسب نظام التشغيل الخاص بجهازك

بعد تعديل الرجستري
قم باعادة تشغيل الجهاز
قم بتشغيل برنامج مكافحة الفيروسات واذا لم يقم بتشغيل نفسه
قم بتحميل المف التالي وهو التحديث الذكي الخاص بازالة هذا الفيروس
.http://securityresponse.symantec.com...download.ht ml

لمستخدمين نظام وندوز **95** و **98** يقوم بالذهاب الى

أبدأ ثم البرامج وبعد ذلك يقوم باختيار ايقونه

MS-DOS

وسوف تفتح لك شاشة الدوس

بعدها انتقل للخطوة الثانية

اما لو كنت تستخدم نظام وندوز ملينيوم

اذهب الى ابدأ ثم برامج بعد ذلك برامج ملحقة ثمMS-DOS

اما بخصوص مستخدمين وندوز ان تي و 2000
فقم بالذهاب الى ابدأ ثم تشغيل واكتب
command
واضغط ok وبعدها راح تنفتح لك شاشة الدوس
أكتب فيها الامر التالي
cd \winnt
ثم انتقل للخطوة الثانية
لو كنت تستخدم وندوز اكس بي
فقم بالذهاب الى ابدأ ثم تشغيل واكتب
command
واضغط okوبعدها راح تنفتح لك شاشة الدوس
أكتب فيها الامر التالي
cd \windows
الخطوة الثانية قم بكتابة الأمر التالي
copy regedit.exe reg.com
اضغط انتر
ثم اكتب الامر التالي
start reg.com
وأنتر
بعد اتمام هذه العملية عليك ان تقوم بتعديل الرجستري وذلك حسب الخطوات التالية
HKEY_LOCAL_MACHINE\Software\Classes\exefile\shell\open\command
اذهب على تشغيل
RUN
اكتب فيها
REGEDIT
واحفظ ملف الرجستي القديم
ولحفظه نذهب لكلمة لكلمة رجستري ونضغط على اكسبورت رجستري فايل وتحفظ الملف في مكان جيد ثم االختار
HKEY_LOCAL_MACHINE
ثم
Software
بعد كذا
Classes
ثم
exefile

ثم
shell
ثم
open
ثم
command
وبعدها دبل كلك على كلم **ديفولت وغير القيمة الموجودة للقيمة هذه**
"%1" %*
وهية
علامة تنصيص + علامة المئوية +رقم واحد + علامة تنصيص +مسافة + علامة مئوية+ نجمة

بالنسبة لوندوز 95 و 98 ووندوزيسوف تكون هذه القيمة موجودة اول ما تضغط على زر الاوكي وسوف تظهر بهذا الشكل
""%1" %*"
نلاحظ علامة تنصيص زايدة وهذه ما راح تظهر لو كان نظام التشغيل
الوندوز 2000 والاكس بي
بعد كذا روح واتاكد من مجلدات الرجستري هذه

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

وبنفس الطريقة السابق ةتستطيع ان تصل لها

HKEY_LOCAL_MACHINE
ثم
Software\Microsoft
ثم
Windows
ثم
CurrentVersion
ثم
Run
وتتاكد اذا
من حذف هذه القيم من الجهة اليمين
WinServices.exe C:\%System%\WinServices.exe

وبعد ذ لك نقوم باعادة تشغيل الجهاز.

حذف فايروس temp1.exe و rose.exe وtemp2.exe

ينشئ هذا الفيروس ملفات وتطبيقات في النظام وفي القسم C وعلى باقي اقسام الهارد أن وجد اقسام

على اقسام الهارد وعلى القسم الذي عليه النظام ينشئ هذه الملفات

C:\copy.exe
C:\host.exe
C:\autorun.inf

في مجلد الوندوز

C:\Windows

ينشئ هذا التطبيق

svchost.exe
xcopy.exe

في مجلد النظام

System32

ينشئ هذه التطبيقات

temp1.exe
rose.exe
temp2.exe

طريقة التخلص من الفيروس

أعد تشغيل الجهاز وأدخل من الوضع الآمنSafe Mode

بمجرد تشغيل الجهاز تبدأ بالضغط على F8

ومن الشاشة تختار الخيار الاولSafe Mode

أظهر الملفات المخفية

طريقة عرض الملفات المخفية
من سطح المكتب
جهاز الكمبيوتر
أفتحه
من أدوات Tools
أعدادات المجلد Folder Options
ثم من تبويب عرضView

ثم نضع العلامة أمام

Show hidden files and folders

ونزيل علامة الصح من أمام

Hide protected operating system files

ثم تطبيق Apply

موافق OK

أفتح مجلد الوندوز

C:\WINDOWS

ثم أبحث عن هذا التطبيق أو المجلد واحذفه

svchost.exe
cxcopy.exe

أفتح مجلد النظام 32

System32

ثم أبحث عن هذا المجلد أو التطبيق وأحذفه

temp1.exe

rose.exe
temp2.exe

طريقة حذف فايروس Win32.Perlovga.a

ينشئ هذا الفيروس ملفات وتطبيقات في النظام وفي القسم C وعلى باقي اقسام الهارد أن وجد اقسام

على اقسام الهارد وعلى القسم الذي عليه النظام ينشئ هذه الملفات

C:\copy.exe
C:\host.exe
C:\autorun.inf

في مجلد الوندوز

C:\Windows

ينشئ هذا التطبيق

svchost.exe
xcopy.exe

في مجلد النظام

System32

ينشئ هذه التطبيقات

temp1.exe
rose.exe
temp2.exe

طريقة التخلص من الفيروس

أعد تشغيل الجهاز وأدخل من الوضع الآمنSafe Mode

بمجرد تشغيل الجهاز تبدأ بالضغط على F8

ومن الشاشة تختار الخيار الاولSafe Mode

```
Windows Advanced Options Menu
Please select an option:

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable VGA Mode
    Last Known Good Configuration
    Directory Services Restore Mode (Windows domain controllers only)
    Debugging Mode

    Boot Normally

Use ↑ and ↓ to move the highlight to your choice.
Press Enter to choose.
```

============= ======

أظهر الملفات المخفية

طريقة عرض الملفات المخفية

من سطح المكتب
جهاز الكمبيوتر
أفتحه
من أدوات Tools
أعدادات المجلد Folder Options
ثم من تبويب عرض View

ثم نضع العلامة أمام

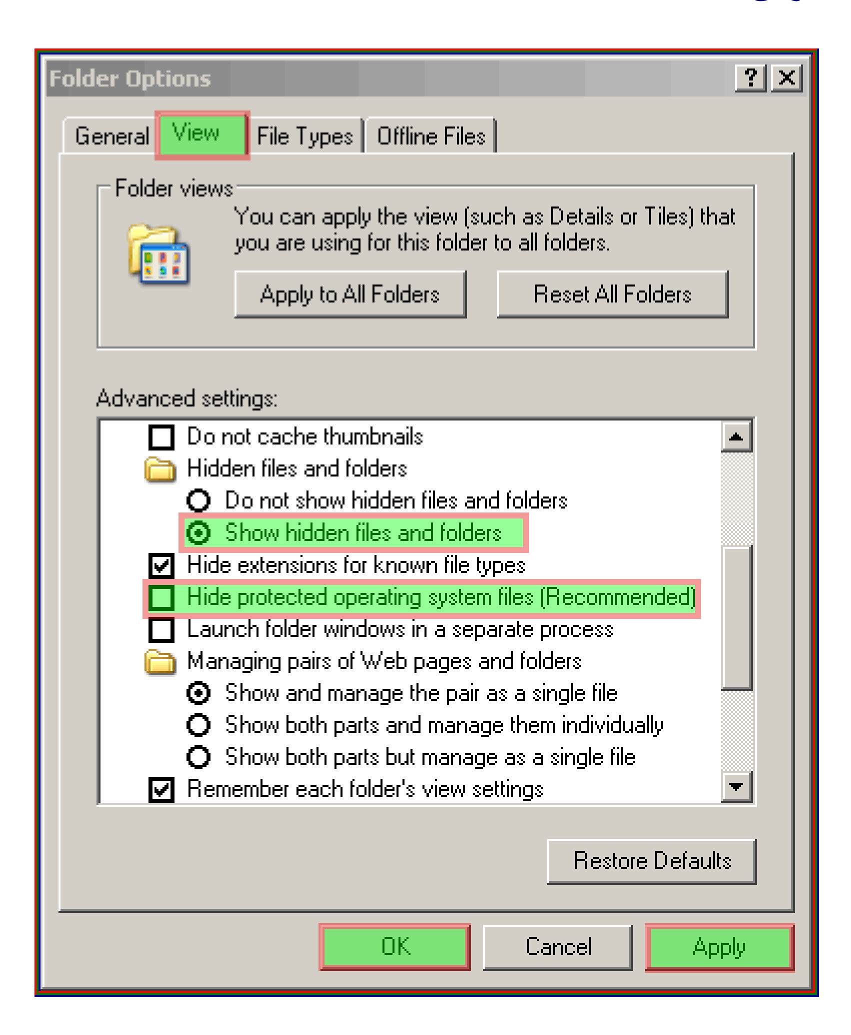
Show hidden files and folders

ونزيل علامة الصح من أمام

Hide protected operating system files

ثم تطبيق Apply

موافق OK



============= =======

أفتح مجلد الوندوز

C:\WINDOWS

ثم أبحث عن هذا التطبيق أو المجلد واحذفه

svchost.exe
cxcopy.exe

============= =======

أفتح مجلد النظام 32

System32

ثم أبحث عن هذا المجلد أو التطبيق وأحذفه

temp1.exe
rose.exe
temp2.exe
============= =======
أفتح القسم C أو القسم الذي قد نصبت النظام عليه

وأحذف هذه التطبيقات
copy.exe
host.exe
autorun.inf
تكرر عملية الحذف لهذه الملفات الثلاث على باقي الاقسام في حال لديك الهارد مقسم الى عدة أقسام
============= =======
أفتح محرر الرجستري تتبع هذا المسار
HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>
Windows>CurrentVersion>Run
من جهة اليمين احذف هذه القيمة
dll = "C:\system32\ rose.exe
حمل هذه الملفات

Perlovga_Fix_ Reg

http://www.ksa-7be.com/up/download3....043939dd02.zip

fix_reg_copy- exe

http://www.ksa-7be.com/up/download3....be4856ce7c.zip
فك الضغط عنها

شغل الملف Perlovga

ثم شغل الملف fix_reg_copy- exe
============= =======
حمل برنامج hijackthis

http://www.ksa-7be.com/up/download3....d695758487.zip

أفحص الجهاز ببرنامج hijackthis وتتخلص من هذه القيم بوضعك علامة الصح امامها ثم الضغط على
Fix checked

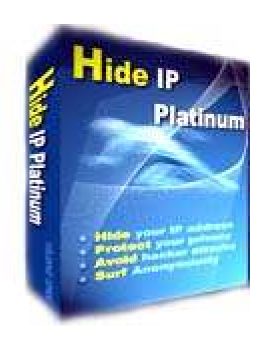
F2 - REG:system.ini: Shell=explorer. exe svchost.exe

الفصل الثاني

((التخفي))

Hide IP Platinum 2.82

برنامج ممتاز جدا يخفي عنوان الاى بى IP أثناء تصفحك على الإنترنت وبذلك فهو يضمن لك الخصوصية التامة - سهل الاستخدام بمجرد التشغيل يعمل البرنامج.



تحميل البرنامج :
http://v7soft.net/download/hideippla.exe
متوافق مع جميع انظمة ويندوز
حجم البرنامج : Kb762.00
الترخيص Shareware :

اخفاء الاي بي بدون برامج

طريقه اخفاء الاي بي الخاص لجهازك

بطريقه سهله من غير برنامج..

أولاً : الأي بي (IP) هو رقم جهازك علي الشبكة العنكبوتية

ويعتمد الهاكرز كلياً علي رقم الأي بي في إختراق الأجهزة

لأكن تستطيع إخفاء هذه الآي بي باتباع التالي:

- 1إضغط على قائمة إبدأ Start
- 2إختار تشغيل Run
- 3ثم أكتب Command ثم إضغط موافق Ok
- 4أكتب الأمر الأتى drwatson ثم إضغط Enter

ستظهر لك أيقونه بالأسفل فى شريط المهام ل dr watson

هكذا لن يستطيع أحد من معرفة رقم الآي لجهازكم

الفصل الثالث

((امن المعلومات))

أمن المعلومات والإنترنت

الإنترنت سلاح ذو حدين، فهو مدخل للكثير من الأشياء النافعة، ولكن مع الأسف، فهو يفتح المجال أمام الكثير من الأشياء المؤذية للدخول إلى جهازك. وثمة العديد من المسائل الأمنية الواجب الاعتناء بها للإبقاء على سلاسة تشغيل أجهزة الكمبيوتر والشبكات. وسنناقش في هذا المقال أهم القضايا الأمنية وبعض الحلول لها.

1. ما هو أمن المعلومات؟

يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة.
أنت بالتأكيد لا ترغب أن يكون للآخرين مدخلاً لمعلوماتك الخاصة. ومن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكن الآخرين من الوصول إليها، والكثير من الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم فإنها قد تعني الكثير لأناس آخرين وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات .فعلى سبيل المثال، يمكن للشركة الراغبة في الحصول على معلومات شخصية عنك للأغراض التسويقية أن تشتري هذه المعلومات من شخص يقوم بتجميعها من خلال الوصول إلى جهاز كمبيوترك بشكل غير شرعي.
ومن المهم كذلك أن تفهم أنك حتى ولو لم تقم بإعطاء معلوماتك لأي شخص عبر الإنترنت، فقد يتمكن بعض الأشخاص من الوصول إلى نظام الكمبيوتر لديك للحصول على المعلومات التي يحتاجونها دون علم أو إذن منك.

2.مواطن الضعف في شبكة الإنترنت

تعتبر شبكة الإنترنت عرضة للعيوب والضعف في دفاعاتها. وقد يكون هذا الضعف ناجما عن الأخطاء البرمجية والعيوب في تصميم النظام. ويعود سبب بعض نقاط الضعف إلى الإدخال الخاطئ للبيانات، حيث أن غالبا ما يسمح بتنفيذ الأوامر المباشرة أو عبارات لغة .SQL وأحيانا يخفق المبرمج في التحقق من حجم البيانات المخزنة، حيث يؤدي ذلك إلى فيض من البيانات والذي يسبب فساد المكدس أو مناطق الشجرة الثنائية في الذاكرة.
وغالبا ما تتيح مواطن الضعف للمهاجم إمكانية التحايل على البرنامج بتجاوز فحص إمكانية الوصول أو تنفيذ الأوامر على النظام المضيف لهذا البرنامج.
هناك عدد من نقاط الضعف والتي يكون جهازك أو شبكتك عرضة لها. ومن أكثرها شيوعا هي أخطاء تدقيق صحة إدخال البيانات مثل الأخطاء البرمجية الناجمة عن تنسيق الرموز النصية، والتعامل الخاطئ مع الرموز المتغيرة لغلاف البرنامج ولذلك يتم تفسير هذه الرموز، وإدخال عبارات SQL وتضمين النصوص البرمجية متعارضة-الموقع داخل تطبيقات الويب. ومن نقاط الضعف الشائعة أيضا تحطم المكدس وفيض البيانات في ذاكرة التخزين المؤقت بالإضافة إلى ملفات الروابط الرمزية.(Symlinks)

فحص مواطن الضعف

يمكن أن تكون هناك نقاط ضعف في جميع أنظمة التشغيل مثل الويندوز، ماكنتوش، لينوكس، OpenVMS، وغيرها. ويمكن فحص نقاط الضعف في الشبكة والخوادم من خلال إجراء اختبار خاص عليها يتم من خلاله فحص الخوادم والصفحات الإلكترونية وجدران النار وغير ذلك لمعرفة مدى تعرضها لنقاط الضعف. ويمكن تنزيل برامج فحص نقاط الضعف من الإنترنت.

3.المشاكل الأمنية

تحدث المشكلة الأمنية عندما يتم اختراق النظام لديك من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة.
وأكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت، حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة. ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم.
وفي حالة وجود أخطاء برمجة أو إعدادات خاطئة في خادم الويب، فمن الجائز أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام. كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم تعديل النظام وإطلاق هجمات إغراقية مما يؤدي إلى تعطل الجهاز مؤقتاً، كما أن الهجمات الإغراقية (DoS)تستهدف إبطا او شل حركة مرور البيانات عبر الشبكة. كما أنه من خلال الهجمات الإغراقية الموزعة(DDoS) ، فإن المعتدي يقوم باستخدام عدد من الكمبيوترات التي سيطر عليها للهجوم على كمبيوتر أو كمبيوترات أخرى. ويتم تركيب البرنامج الرئيسي للهجمات الإغراقية الموزعة (DDoS) في أحد أجهزة الكمبيوتر مستخدماً حساباً مسروقاً.
إن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة.

الهاكر

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي. وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة. غير أن هذا المصطلح (هاكر) يمكن أن يطلق على الشخص الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة أنظمة الكمبيوتر وما يتعلق بأمن الكمبيوتر.

فيروسات الكمبيوتر

فيروسات الكمبيوتر هي الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات .وفيروس الكمبيوتر هو برنامج غير مرغوب فيه ويدخل إلى الجهاز دون إذن ويقوم بإدخال نسخ من نفسه في برامج الكمبيوتر، والفيروس هو أحد البرامج الخبيثة أو المتطفلة .والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.
يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطئيه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق

المختلفة التي قد يرغب المستخدم في الدخول إليها. أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك.
أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة. كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.
يمكنك حماية كمبيوترك وحماية نفسك باستخدام برامج مناسبة لمكافحة البرامج الخبيثة غير المرغوب فيها والتي قد تكون نتائجها مدمرة. للمزيد من المعلومات، إطلع على" كيف تحمي كمبيوترك من الفيروسات؟ ".

اللصوصية(Phishing)

يستخدم مصطلح (Phishing) للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول الى الموقع.
هناك برامج لمكافحة اللصوصية Phishing والكشف عن هوية المرسل الحقيقي، وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظاً وحذراً ولديه الوعي الكافي، فلا يوجد هناك أي بنك معروف أو مؤسسة فعلية يطلبون من عملائهم إرسال معلوماتهم الشخصية عبر البريد الإلكتروني.

البريد الإلكتروني

يجدر بنا أن نتذكر دائماً إلى أن البريد الإلكتروني لا يضمن الخصوصية، فخصوصيته تشابه خصوصية البطاقة البريدية. ويتنقل البريد الإلكتروني في طريقه إلى المستلم عبر العديد من الخوادم حيث يمكن الوصول إليه من قبل الأشخاص الذين يديرون النظام ومن الأشخاص الذين يتسللون إليه بشكل غير نظامي.
والطريقة الوحيدة للتأكد إلى حد ما من خصوصية بريدك الإلكتروني هو تشفيره.
انظر الفقرات التالية..

حتى إذا شعرت أن أحد ما تمكن من الوصول إليها. ولا تكتب كلمات المرور الخاصة بك في أي مكان ولكن عليك أن تتذكرها بنفسك.

التحديثات

حافظ على تحديث جميع برامجك بما في ذلك أحدث نسخة من برنامج التشغيل الذي تستخدمه. وإذا كنت تستخدم التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز، فعليك إعادة تشغيل جهازك يومياً.

جدار النار(Firewall)

يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادم من المتسللين. وتختلف جدران النار حسب احتياجات المستخدم. فإذا استدعت الحاجة إلى وضع جدار النار على عقدة منفردة عاملة على شبكة واحدة فإن جدار النار الشخصي هو الخيار المناسب. وفي حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتم استخدام مصافي لجدار النار في الشبكة لتصفية جميع الحركة المرورية. علماً بأن

.4كيف تحمي شبكتك ونظامك

عليك بالحذر والحرص الدائمين لحماية نظامك كي لا يكون عرضة للهجمات بسبب نقاط الضعف فيه، ويمكنك تركيب برامج فعالة لجعل استخدام الإنترنت أكثر أماناً لك.

وسائل الحماية الماديةسنستعرض في الفقرات التالية المزيد من المعلومات حول البرمجيات المختلفة والوسائل المتعلقة بالأنظمة الأخرى للإبقاء على معلوماتك آمنة، لكن علينا أن نتذكر أن ثمة العديد من الطرق الأخرى التي يسلكها المتسللون للوصول إلى معلوماتك. ضع كمبيوترك وخصوصاً الكمبيوتر المحمول دائماً في مكان آمن. قم بحماية كمبيوترك بكلمة مرور ويستحسن أن تطفئه وأنت بعيداً عنه. عليك أن تشك في أي شخص يرغب في الحصول على أي من كلمات المرور الخاصة بك، حتى أولئك الأشخاص الذي يعملون (أو يدعون بأنهم يعملون) في الدعم الفني في شركتك. فإن أرادوا الحصول على كلمة المرور الخاصة بك، قم أنت بطباعتها (إدخالها) بنفسك (بحيث لا يرونها) ولا تبلغها لهم شفوياً أو خطيا. قم بانتظام بتغيير كلمة المرور إذا تصادف أن اطلع عليها أحد غيرك، أو

الكثير من الشبكات والخوادم تأتي مع نظام جدار نار افتراضي، ولكن ينبغي التأكد فيما إذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي تحتاج إليها، فإن لم يكن قادراً على ذلك، فينبغي شراء جدار حماية ناري أقوى منه.

برامج مراقبة بيانات الشبكةPacket Sniffers

طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة.

التشفير

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن .ومن أشهر برامج التشفير (PGP) الموجود على الرابط التالي .http://www.pgp.com/

5.أمن الشبكة اللاسلكية

تنتشر الشبكات اللاسلكية في كل مكان وتنمو بشكل غير طبيعي ولا توجد دلالات على توقف ذلك النمو على **المستوى المنظور. وهناك العديد من القضايا الأمنية المصاحبة لهذه الشبكات اللاسلكية، كما أن بإمكان أي شخص الوصول إلى الشبكة اللاسلكية من أي مكان تتوفر فيه الوصلة اللاسلكية. وبالإضافة إلى التدابير الأمنية العامة المتبعة لحماية الشبكات اللاسلكية، فإنه من الضروري اتباع المبادئ العامة البسيطة لتوفير أفضل مستوى من الأمن لشبكتك اللاسلكية.**

التشفير

يتم حماية الشبكة اللاسلكية باستخدام بروتوكول تشفير الشبكات اللاسلكية .(WEP) ويعمل هذا البروتوكول بتضمين مفتاح مشترك 64 أو 128 بت بين العملاء ونقطة الدخول، ومن ثم يتم استخدام هذا المفتاح لتشفير وفك تشفير البيانات بينهم، وهذا يوفر قدر كاف من الأمن للشبكات المنزلية. عليك الرجوع إلى الوثائق الخاصة بالأجهزة اللاسلكية لديك لتعرف كيفية تمكين وإعداد بروتوكول التشفير اللاسلكي (WEP) على شبكتك. أما بالنسبة لبيئات الشركات، فيجب اعتبار هذا البروتوكول (WEP) فقط كنقطة بداية للترتيبات الأمنية، وعلى الشركات البحث جدياً في ترقية شبكاتهم اللاسلكية إلى مستوى (WPA) أكثر أماناً.

التعريف

يكون للأجهزة ومديرو الشبكات أسماء تعريف افتراضية في النظام، ومن السهل كثيراً على الهاكر إيجاد هذه الأسماء، ومن ثم عمل كلمات مرور واسم مستخدم شخصي لك من خلال تعديل أسماء التعريف الافتراضية في النظام. لذا ننصح بإعطاء الأجهزة لديك أسماء لا تكشف عن هوية صاحبها أو أماكنها، ومثال ذلك بدلاً من استخدام عنوانك الفعلي مثل اسم المبنى أو اسم الشركة كأسماء لأجهزتك، يمكنك استخدام أسماء مختلفة مثل "الجبل "Mountain أو "جهازي."My Device

الإعلان عن المعرفIdentifier Broadcasting قد يكون في جهازك وظيفة افتراضية لبث (الإعلان عن) حالة التوصيلة، وحيث أنه قد يكون سهلاً على الهاكرز اختراق الشبكة اللاسلكية، لذا عليك تعطيل عمل خاصية الإعلان عن المعرف.Identifier broadcasting

ترشيح العناوينMAC filtering يعرف عنوان (MAC) كذلك بأنه العنوان المادي، وهو معرف فريد لكل جهاز في الشبكة .ويعني مصطلح ترشيح العناوين أن تقوم يدوياً بإدخال قائمة بالعناوين الموجودة في شبكتك المحلية وتقوم بإعداد الموجه لديك (router) ليسمح فقط بتوصيل هذه العنوانين المحددة عبر الشبكة اللاسلكية. ويمكن بسهولة العثور على العناوين (MAC Addresses)من خلال الذهاب إلى مؤشر الأوامر (Command Prompt) في كل نظام وكتابة هذه العبارة:

```
ipconfig /all
```

الخلاصة

يمكنك من خلال اتباع هذه التدابير والتعليمات الأمنية جعل شبكتك واستخدامك للإنترنت أكثر أماناً. ونظراً لأن تقنيات وأساليب الهاكرز والمتسللين الآخرين تتطور مع مرور الزمن، لذا فإن عليك تثقيف نفسك باستمرار من خلال متابعة المعلومات الأمنية ضمن المواقع الإلكترونية التي تقدمها. (انظر على سبيل المثال منتدى أمن

المعلومات على الرابط التالي http://www.securityforum.org/.

حماية المعلومات البنكيه

- كن حذرا من الدخول على الانترنت في الأماكن العامة
تجنب الدخول على حسابك البنكي في مقاهي الانترنت والمكتبات والأماكن العامة الأخرى لتجنب مخاطر نسخ معلوماتك الشخصية وسوء استخدامها بعد مغادرتك المكان.
- كن على دراية بالتزوير على الانترنت
اعلم بأن هناك عدد من المواقع الخداعة على الانترنت وتم تصميمها لخداعك من أجل الحصول على بيانات شخصية. وفي بعض الأحيان, تكون وصلات هذه المواقع في رسالة الكترونية من المفترض أن تكون مرسلة من مؤسسات مالية. كن على يقين من أنك تستخدم عنوان الموقع الرسمي المعروف للدخول على صفحات البنك. وبنك كريدي أجريكول مصر لن يقوم مطلقا بإرسال مثل هذه الرسائل لك.
- تغيير كلمة السر الخاصة بك
عليك بتغيير كلمة السر التي قد تعرضك للخطر. ونوصيك بتغيير كلمة السر الخاصة بك على فترات منتظمة.
- اتصل بالبنك إذا اعتقدت أن شخصا آخر يعرف كلمة السر الخاصة للدخول لحسابك على الانترنت
- حماية حاسبك عن طريق كلمة سر
استخدم كلمة سر خاصة بجهاز الحاسب عندك لمنع دخول أي شخص دون إذن على الجهاز والاطلاع على بياناتك.
- قم بتعطيل وظيفة "التكامل التلقائي" داخل المتصفح
سوف يعمل هذا على منع الآخرين من الاطلاع على بياناتك الشخصية. في متصفح الانترنت, على سبيل المثال, تستطيع وظيفة "التكامل التلقائي" تذكر البيانات التي قمت بإدخالها وفي بعض الأحيان قد تتضمن كلمات السر.

<u>حافظ على سرية كلمة السر</u>

تعد كلمة السر هي مفتاح الدخول للمعلومات الخاصة بحسابك وأرصدتك على الانترنت, و المشاركة في أية نشاطات على الانترنت. فكلا من كلمة السر الخاصة بك للدخول على حسابك الخاص لبنك كريدي أجريكول مصر إضافة إلى بيانات الهوية هي التي تسمح بدخولك لحسابك البنكي على الانترنت. ولذا فينبغي أن تكون كلمة السر الخاصة بك فريدة وتتمتع بالحماية الجيدة جدا.

نصائح هامة

- احتفظ بكلمة السر لنفسك ولا تعطيها لأي شخص
- **اجعلها كلمة سر متميزة**, حاول أن تكون كلمة السر التي تختارها متميزة ولا يمكن تخمينها بسهولة.
- **استخدم الحروف والأرقام والرموز**, تعد كلمات السر التي تحتوي على حروف وأرقام ورموز مكتوبة لأعلى وأسفل بعيدة بشكل كبير عن التخمين.
- **لا تكتب كلمة السر مطلقا**, وإذا كنت في حاجة ماسة لتسجيلها, فقم بكتابتها بأسلوب الشفرات.

لن يسألك أي شخص في بنك كريدي أجريكول مصر عن كلمة السر التي تدخل بها لحسابك على الانترنت. وإذا سألك أحد عنها فاعلم أنه لا يمثل بنك كريدي أجريكول مصر.

حافظ على حماية جهاز الحاسب الخاص بك

يقدم الانترنت فرصة للقراصنة للدخول على نظامك. وحقيقة على الرغم من أن هناك مواقع وتعد وسيلة هامة للحصول على برامج السوفت وير وتحميل بعض البرامج والموسيقي التي قد تريدها, فإنك عند قيامك بدخول هذه المواقع فإنك تعرض نفسك للخطر. من فضلك, تأكد من أنك تستخدم القواعد الهامة لحماية جهازك.

<u>حافظ على وضع الحماية لحاسبك البنكي</u>

الدخول

تأكد من إدخالك كلمة السر الصحيحة دون أية تفاصيل قد يتم الوصول إليها بغير قصد من أي شخص يحاول الاستفادة منها.

الاغلاق

تذكر دائما أن تقوم بإغلاق صفحة البنك وغلق المتصفح عند انتهائك من تصفح حسابك البنكي. وسوف يساعد ذلك على مسح كافة الخطوات التي قمت بها لزيارة الموقع من ذاكرة حاسبك الشخصي.

نصيحه مهمه

هناك مواقع تبدو أصلية تم تصميمها على أيدى
المزيفون وتبدو مثل المواقع المحترمة الأخرى مثل
موقع الهوتميل اوالياهو مثلا. وهي تجذب عددا من
الأشخاص لمواقعهم من خلال **تصيد** البريد الألكتروني
ودائم ما يطلبون معلومات شخصية سرية
فأحذر من تسجيلها .

الفصل الرابع
((حماية الايميل))

رسالة كاذبة تحذر من فايروس SULFNBK عبر البريد الإلكتروني

أصدرت خدمة دعم المنتجات في مايكروسوفت ، نصيحة لمستخدمي الكومبيوتر في الشرق الأوسط نتيجة للتوزيع الكبير عبر البريد الإلكتروني لرسالة فيروس خادعة. الخبر المضلل نشر أيضا في بعض الأنباء المحلية في المنطقة ونتج عنه شكوك المستخدمين .

نسخ عديدة من رسالة خادعة انتشرت عبر البريد الالكتروني في المنطقة تنبه الى وجود فيروس في الكمبيوتر الشخصي. تفيد الرسالة الإلكترونية إلى أن الملف sulfnbk.exeيحتوي على فيروس وتنصح بمحي الملف من الكمبيوتر على الفور . هذه الرسالة خادعة أن ملف 'sulfnbk.exe' هو جزء من نظام تشغيل ويندوز 98 ويساعد المستخدمين على استعمال الملفات ذات الأسماء الطويلة. إن هذا الملف موجود في أي كومبيوتر محمل بنسخة أصلية أو محدّثة من نظام التشغيل ويندوز 98 وهذا طبيعي .

إذا كنت من مستخدمي ويندوز 98، ويندوز أن. تي، ويندوز أم.أي أو ويندوز2000 و محوت الملف نتيجة لتجاوبك مع تعليمات الرسالة الالكترونية فلا داع للقلق. إن نظام ويندوز يعتمد على هذا الملف في ادارة الملفات ذات الأسماء الطويلة في حال أراد المستخدم الرجوع الى نسخة ويندوز 95. اذا محوت الملف وأردت استرجاع نسخة ويندوز 95، اعادة تحميل الكمبيوتر من جديد بويندوز 98 الحاوي على الملف 'sulfnbk.exe'.

ما العمل؟

إذا وصلتك الرسالة الإلكترونية لا تتجاوب مع تعليمات الرسالة. إن الرسالة خادعة. لا تبعث الرسالة لأصدقائك و معارفك. إذا تجاوبت مع الرسالة واتبعت التعليمات منها ان محو ملف 'sulfnbk.exe' لن يؤثر على معظم النظم المستخدمة اليوم لأن 'sulfnbk.exe'هو جزء من نظام تشغيل ويندوز98 ويساعد المستخدمين على استعمال الملفات ذات الأسماء فقط في حالة رجوع المستخدم من نظام ويندوز98 إلى نظام ويندوز95. إن معظم المستخدمين اليوم ليسوا بحاجة إلى هذه الميزة . لأي شكوك عن فيروسات و تنبيهات عن الفيروسات يجب على أي مستخدم تحميل الكمبيوتر بنظام كاشف للفيروسات معروفا و معتمدا ويجب تحديث هذا النظام دوريا. هناك العديد من منتجي هذه البرامج. باستطاعتك البحث والتحقق من تنبيهات المتعلقة بفيروسات الكمبيوتر عبر صفحات منتجي البرامج المضادة للفيروسات على الانترنت ومنهم سيمنتك www.symantec.com or www.sarc.com أو نتورك أسوشيتس www.mcafee.com.

((كيف تصنع كلمة سر؟))

ان تكون كلمة المرور طويلة جدا , لأن البعض يجعل خانات كلمة المرور عبارة عن خمس او سبع خانات والافضل ان تجعلها اكثر من عشرين خانة.

- 2ان تحتوي كلمة المرور على خليط من الرموز , الأرقام و الحروف مثال
19MYO~QM/+-^%BO*ZP37

- 3ان لا تضع كلمة المرور بسيطة الادخال على لوحة المفاتيح حتى وان اشتملة على النقطتين السابقتين 1 - 2 لأن البعض يجعل كلمة المرور بهذا الشكل
~!@#$%^&*QWERTYUIOP123
لا حظوا ادخلنا الرموز اولا بالترتيب لأنها في الجزء الاعلى من لوحة المفاتيح ثم ادخلنا الاحرف التي اسفل من الرموز في لوحة المفاتيح ايضا بالترتيب ثم ادخلنا الارقام مرتبة , والافضل التنقل في جميع اجزاء لوحة المفاتيح بشكل عشوائي حتى يصعب تخمينا او قد يتمكن شخص من الحصول على كلمة المرور بضربة حظ . !

- 4ان لا تكون كلمة المرور عبارة عن ارقام تسلسلية او ارقام عشوائية قد تراها انت صعبة لكن سهلة عندما يكون هناك برنامج لأنتاج الارقام سواء تسلسلية او عشوائية مهما طالة الخانات . والبعض يستخدم ارقام تسلسلية مثل
123456789او 1223334444 او 102030405060 والكثير من هذه الامثلة والبعض يستخدم كلمات مرور بهذا الشكل بكل ثقه . !

- 5ان تكون كلمة المرور بعيدة جدا عن أي معلومة حقيقية تخصك مثل رقم الهاتف اسمك اسم المدينة الدولة التي تسكنها تاريخ ميلادك لأن البعض يجعل كلمة المرور بأسم الدولة او المدينة ثم يتبعها بتاريخ الميلاد وهكذا وايضا ان تبعدها عن أي معلومة معروفه عنك في منتدى تشارك فيه حتى ولو كانت تلك المعلومة تخص اسمك المستعار.

- 6ان تكون كلمة المرور بعيدة عن الأسماء المشهورة وايضا الأجنبية مثل اسم لاعب او اسم مغني لأن مثل هذه الكلمات تكون قريبة للفكر والتخمين اكثر ولأن هناك برامج تعتمد في عملها على ملفات بها كلمات مرور اجنبية تقوم بتجربتها على البريد , ايضا تسمح هذه البرامج بأضافة كلمات مرور اخرى ضمن قائمتها او قد يخصص قائمة لهذا البريد بهدف سرقته فيضع جميع الكلمات التي يتوقعها.

- 7ان تثق في الشخص الذي تراسله لأنه بعد فترة من الزمن من الاخذ والعطاء يستطيع جمع معلومات عنك قد تفيده في كشف كلمة المرور.

- 8ان لاتجعل كلمة المرور هي اسم مُرسل البريد لأنها قد تفيد حتى وأن اتبعتها بأضافة بسيطة ليست معروفه . لأن البعض يكون اسمه **snowfall** الذي ادرجه عند تسجيل البريد فيضيف اسم البريد مع اسم الُمرسل وتكون كلمة المرور بهذا الشكل
Snowfallsnowfallitgo
orsnowfallsnowfallitgoyahoocom

- 9تغيير كلمة المرور بين فترة وأخرى لأنه ربما يكون هناك شخص استولى

بالفعل على البريد لكن لم يغير كلمة المرور ينتظر ان تصل لبريدك رسائل مهمه او قد يتصف بالجاسوسية يريد ان يتعرف عليك اكثر ! ولتأ كد ان الرسالة لم تقرء تجد شريط عنوان الرسالة نشط واذا قرءة الرسالة تجد تغير في لون عنوان الرسالة أي غير نشط .

- 10ان تكتفي ببريد واحد او اثنان وان تجعل لكل واحد منهما كلمة مرور مختلفة لأن البعض من كثرة ما يملك من حسابات بريدية يتكاسل ويجعل لها كلمة مرور واحدة فأذا سُرِق أي بريد منها سوف يفقد بقيتها.

- 11اذا كنت تملك كلمات مرور صعبة التذكر لطولها او لأشتمالها على خليط من الرموز , الارقام والحروف وصعبة الحفظ والتذكر سواء كانت لبريد لبطاقة بنكية او لمنتدى لا تجعل لها ملف خاص داخل الجهاز أكتبها في ورقة خارجية والصقها بالقرب من الجهاز او اكتبها في نوتة الأرقام الهاتفيه اكتبها في مكان آمن بعيدا عن الجهاز.

- 12اذا كنت تشارك بمنتدى اجعل بريدك المعروف لأعضاء المنتدى وزواره للأختبار فقط أي لا تجعله البريد الأساسي اوالشخصي الذي تستقبل فيه معلومات خاصه وحقيقية عنك مثل ان تراسل زوجتك او اشخاص بينك وبينهم امور شخصية على هذا البريد.

- 13يجب ان تكون حذر جدا عند استخدام الماسينجر وان تثق في الشخص الذي تتحدث معه لأنه لو طلب منك ان تتحدث معه بالصوت يستطيع ان يحدد رقم الأي بي الخاص بك أثناء التحادث ويستخدم بعد ذلك برنامج كراكرز في الوصول لجهازك مباشرة وهناك الكثير فقد السيطرة على بريده بعد استخدامه للماسينجر وحتى وان كانت المحادثة نصية , ايضا البعض يدخل لحسابه البريدي من خلال الماسينجر ويطلب من الماسنجر ان يحفظ كلمة المرور والأفضل الدخول للبريد من الموقع , ايضا هناك برامج متخصصه في الحصول على كلمات المرور وتعمل هذه البرامج اثناء استخدام الماسينجر. !

- 14الابتعاد عن مواقع البريد المشهورة وحاول بقدر المستطاع ان تأخذ لك حساب بريدي في مواقع ليست مشهورة لأن معظم الطرق والبرامج المستخدمة والتجارب في الحصول على كلمات المرور جميعها واغلبها موجهه لهذه المواقع مثل موقع الهوت ميل وهذا ملاحظ وكثير ما نسمع من فقد كلمة مرور حسابه البريدي في هذا الموقع وايضا بريد****** ه مع انها تقدم خدمات قد لا نجدها في مواقع أخرى و مستوى الأمن بها عالي ولأفضل الابتعاد عنها هذا من وجهة نظري

- 15الأبتعاد عن المواقع الشخصية لأن بعض منها تقدم مجال من خلالها أي من خلال الصفحة لدخول الي حساب بريدك مثل بريد الهوت ميل او******ه او أي بريد آخر ونجد فيها حقل لأسم حساب البريد وحقل لكلمة المرور وفي الحقيقة ما هي إلا طريقة للحصول على كلمة المرور فعندما تريد الدخول لحسابك من خلال هذا الموقع تُرسل معلوماتك لصاحب هذه الصفحة وتقع في فخ ولذلك لا تدخل لبريدك إلا من موقعه الاصلي.

16- تعطيل تشغيل خاصية جافا سكربت لأنها تستخدم في اعادة ادخال معلوماتك من اسم الحساب وكلمة المرور لتصل للمستفيد وهي رمز يدرج في الرسالة وعند فتح هذه الرسالة تظهر لك مطالبة بأعادة ادخال معلومات بريدك من اسم الحساب وكلمة مرور وبعد ذلك توجه معلوماتك من اسم الحساب وكلمة مرور للمستفيد وهي تنطبق على أي بريد وللهروب من هذه الرسالة عليك اعادة ادخال بيناتك من حقل الموقع الاصلي وليس من حقل الرسالة الوهمية وهناك طريقة لتعطيل تشغيل جافا سكربت من متصفح الاكسبلورل .

17- لا تجعل جهاز الكمبيوتر يستخدم خاصية الإكمال التلقائي لأن هذه الخاصية عند استخدامها تحتفظ بجميع كلمات المرور التي ادخلتها سواء في بريد او منتدى او بطاقة بنكية داخل الجهاز و الاغلبية منكم قد لاحظ عند كتابته اول حرف من اسم حسابه في البريد او في المنتدى يظهر الاسم مباشرة دون الحاجة لأكمال اسم الحساب وايضا عند ادخال كلمة المرور تظهر كلمة المرور مباشرة في شكل نجوم وهذا دليل على ان اسم حسابك وكلمة المرور يحتفظ بها الجهاز فقد يسيطر على جهازك كركرز ومن المعروف ان معظم برامج الكركرز يوجد بها امر مخصص فقط للحصول على كلمات المرور واسماء الحسابات المخزنة في الجهاز نتيجة خاصية الاكمال التلقائي ولتعطيل خاصية الإكمال التلقائي وهذه نقطة مهمة جدا من متصفح الأكسبلور نختار منه

أدوات

خيارات إنترنت

محتوى

إكمال تلقائي

أزل جميع علامات صح من الخيارات الموجودة اسفل من هذه الجملة استخدام الإكمال التلقائي لـ

عنوين ويب . ازل علامة صح

النماذج . ازل علامة صح

اسماء المستخدم وكلمات المرور في النماذج. ازل علامة صح

المطالبة بحفظ كلمات المرور. ازل علامة صح

اضغط على زر مسح كلمات المرور

اضغط على زر مسح النماذج

ثم موافق.

يجب الأنتباه بعد هذه الاعدادات لأنه سوف تظهر لك رسالة عند الدخول لأي حساب تخبرك هل تريد استخدام الإكمال التلقائي اختر لا . واحتمال كبير ان تستمر معك , ايضا الأنتباه للخيار وغالبا ما نراه في مواقع البريد وبرنامج الماسينجر وهو تذكر كلمة المرور واسم الحساب على هذا الجهاز لا تضع علامة صح على هذا الخيار.

- 18الأبتعاد عن استخدام أي طريقة لأستعادة كلمة المرور التي فقدتها لأنه ربما تكون ضحية للمرة الثانية وعن البرامج المتخصصه في هذا المجال لأن اغلبها عبارة عن تروجين قد تسيء استخدامها وتقع في فخها و الابتعاد ايضا عمن يقول انه يستطيع اعادة كلمة المرور والابتعاد عن المواقع وخصوصا الشخصية التي تدعي انها تعيد كلمة المرور التي فقدتها.

- 19دائما وابدا عند الانتهاء من تصفح بريدك وقرائت الرسائل اختر الامر خروج من حساب البريد Sign Out لأنه عند محاولة الرجوع لصفحة البريد بعد ذلك يتطلب منك ان تدخل كلمة المرور وهذه النقطه مهمة جدا خصوصا لزوار مقاهي الانترنت لأنه لو استخدم شخص آخر الجهاز يستطيع الدخول إلي بريدك .

- 20لأبتعاد عن ارسال روابط المواضيع من خلال الماسينجر وهنا اتكلم للحفاظ على حساب الأشتراك بالمنتديات لأنه عند ارسال رابط لموضوع وانت بالفعل داخل المنتدى بحساب اشتراكك يستطيع مستقبل هذا الرابط ان يضيف مشاركات ومواضيع تحمل اسمك في هذا المنتدى وهي نتيجه لأتصالكم ببعض في نفس اللحظة كما لو كنتم في جهاز واحد ولذلك يجب الخروج الرسمي من المنتدى واكثر المنتديات يوجد بها خيار الخروج لأن وحتى وإن حاول الشخص الذي معك على الماسينجر في نفس اللحظة اضافة موضوع او مشاركة تحمل اسمك بعد استخدامك امر الخروج من المنتدى سوف لن يستطيع ابدا فعل أي شيء لأن الموقع سوف يتطلب منه اسم المستخدم وكلمة المرور , وكثير ما نرى مثل هذه المواقف فنرجوا الانتباه , وايضا هذه النقطة ينتبه لها زوار مقاهي الانترنت .
وهذا برنامج يقوم بمسح ملفات الكوكيز تلقائيا من الجهاز والتي تستخدمها معظم المنتديات في تصفح الموقع دون الحاجه للخروج الرسمي من الموقع وله مهام اخرى واحتمال كبير ان تواجهو مشكله في منتديات PHP بسبب هذا البرنامج أي لا تستطيعو اضافة مشاركة لكن بالساحة ليس هناك مشكلة في استخدامه البرنامج سهل الاستخدام

اسم البرنامج: Ghost Surf Version 1.50

رقم تسجيل البرنامج:

CrazyKnight@gmx.net

12502

- 21ان تتجنب فتح المرفقات الأتيه من طرف مجهول ولو كانت من صديق من يظمن ! لأنها قد تكون عبارة عن تروجين وما ان تفتحها حتى يثبت التروجين بجهازك ويوجد الكثير من هذا التروجين مخصص فقط للبريد للحصول على كلمة

المرور وتوجيهها لبريد المستفيد مباشرة ومنها لأوضح لكم خطورتها يعمل على حفظ أي عملية ادخال تمت على لوحة المفاتيح لأي حساب حتى وان تعطلة خاصية الإكمال التلقائي ! وقد لا يكتشفها برنامج الحماية لأنها ربما تكون مدمجه مع ملف حماية. !

- 22ان تثق في المنتدى الذي تشارك فيه لأن البعض يجعل كلمة مرور البريد هي كلمة مرور حسابه في المنتدى او يكون المسؤل عن المنتدى غير آمن.

- 23عند استيلاء شخص على بريدك ويوجد رسائل مهمة جدا لا تريد ان يطلع عليها مهما كلف الامر من وجهة نظري عليك بستخدام برنامج تدمير البريد لأن مهمة هذا البرنامج هي ارسائل الاف الرسائل للبريد وبذلك يصعب ملاحظة رسائلك المهمة مع الكم الهائل من رسائل تدمير البريد ولا ننسى وضع عناوين مختلف لكل مجموعة رسائل او ان تجعلها بنفس عناوين الرسائل التي لا تريده ان يقرئها.

- 24ابتعد عن ارسال رسالة تتضمن سب او شتم للشخص الذي استولى على بريدك ولا تظهر الاهمية له لأنه ربما يزداد تمسكا به وحاول بعد فتره ان تتملك عاطفة هذا الشخص برسائل من يدري قد يعفوا عن بريدك. !

- 25عند تسجيلك لحساب بريدي لأول مرة لا تكتب معلوماتك الحقيقية في طلب تسجيل البريد فرضا تسكن بالسعودية اختر اسكن بالهند بمدينة كلكتا الأسم جاتندر أي اسم المهم لا تكن معلومات حقيقية . راجع الفقرة 5 - 7- 8

- 26حاول بقدر المستطاع ان تحتفظ بصفحة المعلومات الشخصية لحساب بريدك في Floppy قرص مرن وليس داخل الجهاز لأن الكثير ينسى معلومات التسجيل هذه والتي تتضمن السؤال السري لتفيده بعد ذلك اذا فقد كلمة المرور في مراسلة المسؤل عن موقع البريد لأستعادتها.

- 27التأكد من بريد المسؤل عن الموقع اذا اردة ارسال بياناتك لأستعادة كلمة المرور وتجد البريد الاصلي في صفحة المساعدة من البريد .

- 28حاول بقدر المستطاع ان تزيل جميع الرسائل من البريد اول بأول دائما وابدا ولا تنسو ازالتها نهائيا من ملف FOLDER واذا كان هناك رسائل مهمة اخرجها من البريد واحفظها خارج البريد لأنه لو استولى شخص على البريد يجد البريد فارغ لا يجد ما يغريه ولا يجد أي معلومة تجعله يتمسك بالبريد ويتوقع ان بريدك فارغ وليس له اهمية بالنسبة لك ويتركك وشئنك.!

- 29الكثير منا عند ادخال بياناته في طلب تسجيل بمنتدى او بريد لا بد من ان يضع بريده ضمن متطلبات التسجيل و لكي يستقبل عليه معلومات التسجيل ومن ضمنها كلمات المرور ولذلك من الافضل ان تخصص بريد لهذا الشئن بذلك تفقد البريد ولا تفقد الكثير!

هل بريدك معرض للاختراق ؟؟

قد تكون مهتماً جداً باحتمال اعتراض بريدك الإلكتروني وقراءته من قبل الآخرين، وكذلك يهتم العديد من مستخدمي الإنترنت بذلك. وبشكل فعلي، فهذه الأشياء القليلة التي تحدث ضمن الإنترنت، إذا، هل يستطيع الآخرون اعتراض بريدي الإلكتروني؟

والجواب ببساطة هو" نعم "

ولكن،

هل يستطيع الآخرون اعتراض بريدي الإلكتروني بسهولة،

والجواب هو" لا"

فاعتراض البريد الإلكتروني ضمن الإنترنت يحتاج إلى الجهد والتخطيط المسبق. إن بيانات البريد الإلكتروني يتم نقلها عبر الإنترنت ضمن رزم Packetsوهذا يعني أن رسالة البريد الإلكتروني يتم إرسالها غالباً ضمن مجموعات متعددة ولزيادة التعقيد، فلا يتم إرسالها كل رزمة بنفس المسلك الفعلي للرزم الأخرى. لذلك فأي شخص يريد اعتراض البريد الإلكتروني، يجب أن يمتلك خبرة تقنية عالية إضافة إلى خبرته في الوصول إلى الكمبيوترات وخطوط البيانات التي تتعامل مع الرسائل الإلكترونية، كما أنه يجب عليه أن يبذل مزيداً من الجهد لتعقب الرزم واعتراضها وإعادة تجميعها وهذا يشار إليه عادة بالمصطلح

Packet-sinffing

وهو بحد ذاته تطبيق متوفر بالأنترنت يستغله المخترقون وهنا هو عامل الخطورة لأنه مع وجود التطبيقات المناسبة وانتشارها بالإنترنت، يتوفر عامل يدعم عمليات اعتراض البريد الإلكتروني ويسهل هذه المهمة فلا تحسبن أن الجهد والمشقة سيكونان مضنيين على الراغب بقوة في اعتراض بريدك الإلكتروني واحرص في ذلك على حماية منطقتك الأمنية.

تعلم التشفير الذاتي للارقام السريه

الهدف من هذه الطريقة هي اختيار كلمات صعبة, تحوي ارقاماً و حروفاً كبيرة و صغيرة و في نفس الوقت لن تحتاج الى تذكرها ابداً.

الطريقة هي طريقة التشفير الذاتي, لنأخذ مثال على هذا. لنفرض انني اخترت كلمة السر التالية:

MohammeD1

صحيح انها كلمة ليست صعبة للغاية, لكنها نافعة كبداية, فهي تحوي علىحروف صغيرة و كبيرة و رقم ومجموعهم 9 حروف وهو عدد جيد.

لنفرض انك تملك 10 حسابات و كل حساب لديه كلمة سرية مختلفة تماماً و صعوبتها اصعب من هذه الكلمة, و تريد ان تتذكرها بطريقة سهلة و مناسبة.

هنا يبدأ التشفير الذاتي, يجب ان تتفق مع نفسك على اختيار معادلة معينة , و لتكن المعادلة عبارة عن اضافة رقم 2 بعد كل حرف من حروف الكلمة السرية,بمعنى آخر ستكون الكلمة السرية هي:

M2o2h2a2m2m2e2D212

عند النظر الى هذه الكلمة, ستجد انها مختلفة تماماً عن الكلمة الاصلية! الفرق اننا اضفنا رقم 2 بعد كل حرف من كلمة السر الاصلية.افرض انك كتبتها على ورقة كبيرة بخط كبير جداً ووضعتها امام جهازك, هل سيعلم احد انها الكلمة السرية الخاصة بك؟ لا! وحتى ان علموا, فانهم لن يستطيعوا استخدامها مطلقاً لانها ليست الكلمة السرية الاصلية, بل هي مشّفرة بتشفير معين لا يعلمه احد سواك!
يمكنك تشفيرها باي طريقة تريد, هناك اساليب عديدة, منها اضافة رقمين في نهاية الكلمة السرية كالتالي:

MohammeD231

التشفير هنا سهل, فقد اضفنا رقم 23 الى نهاية الكلمة السرية الاصلية, و ان شاهد احد الناس هذه الكلمة فلن يستطيع معرفة الكلمة الاصلية لانه لا يعلم ان رقم 23 عبارة عن رقم اضافي للتضليل!

يمكنك استخدام الطريقة هذه مع 10 كلمات سرية وكتابتها في ورقة تأخذها معك حيث شئت, و حتى ان ضاعت الورقة فلن يستطيع احدهم معرفة الكلمة السرية الاصلية, لانه سيتوقع ان الكلمة المكتوبة هي اصلا الكلمة السرية, وعند استخدامها لن يتمكن من الدخول! عليك فقط بالمحافظة على سريّة المعادلة التي استخدمتها, فان عرفها احد الناس فيسكشف الطريقة.

تفادي EmailBomber

والEmailBomber هو

ارسال رسائل باللاف دفعه واحده على اميلك ليتم تعطيله بواسطة برامجEmailBomber

وهي كثيرة ويمكن أن تغلق الايميل لفترة معينة .. لا يرسل ولا يستقبل ، ومن هذه البرامج ما يلي:

Stoned Email

Kaboom

Una Bomber

Mail Fraud

Fake Mail

eXtreme Mail

ويمكنك وضع حماية لإ يميلك حتى لا يتأثر بتلك البرامج..

وبطريقة سهلة جدا ، ولكنها خاصة بمن يمتلك ايميلاً علىhotmail

والطريقه هي:

أولاَ: أدخل إميلك

ثانياً : قم بإختيار Options الكلمة الموجوده في الأعلى

ثالثاً : من قائمة mail handling أختر كلمةJunk Mail Filter

رابعاً : ستجد العلامه موجوده على of قم بإختيار high وبإمكانك إختيار low المهم لا تختارof

الآن جرب أن ترسل لنفسك بإحدى هذه البرامج رسائل لتدمير الايميل .. ستجد أنها لا تصل إلى الinbox

ولكنها سوف تصل إلى مجلد ال Junkmail ومهما كان عدد الرسائل المرسلة فلن يتأثر الايميل بها.

نصائح مهمه للحفظ على بريدك

- عليك بحفظ السؤال السري والاجابه السريه لانها تفيدك في استراجاع بريدك االمسروق
- عدم استقبال أي ملف من شخص لا تعرفه او لا تثق به فد يكون (ملف تجسس)
- لا تحتفظ بصورك الخاصه ومعلوماتك الشخصيه او البنكيه في صندوق الوارد وحاول مسحها اول بأول
- تجنب الدخول للمواقع المشبوهه لتحافظ على جهازك خالي من ملفات التجسس
- لاتقم بادخال باسورد ايميلك في أي موقع (يطلب) منك ذالك ماعدا موقع الايميل نفسه
- الحذر من مواقع الايميل المزيفه التي قد تتسبب في اختراق ايميلك بكل (خبث) ومهاره
- حماية البريد من الاغراق والرسائل الكبيره التي تؤثر على الارسال والاستقبال (الطريقه مشروحه بالصفحه رقم 35)
- حاول دائما اغلاق كاميرا الايميل ولا تفتحتها الا في الضروره للتجنب سرقة صورك الخاصه ولا تتحول لعرض مباشر على شاشة المخترق ليسجل منه مايشاء.

اسماء اخطر الفايروسات فتكاً بالايميل

1) buddylst.exe
2) calcul8r.exe
3) deathpr.exe
4) einstein.exe
5) happ.exe
6) girls.exe
7) happy99.exe
8) japanese.exe
9) keypress.exe
10) kitty.exe
11) monday.exe
12) teletubb.exe
13) The Phantom Menace
14) prettypark.exe
15) UP-GRADE INTERNET
16) perrin.exe
17) love You
18) Snow White and the Seven Dwarfs
19) CELCOM Screen Saver or CELSAVER.EX
20) Win a Holiday (e-mail)
21) JOIN THE CREW 0 PENPALS Subject: Virus

لاحظ ان امتدادها هو (exe)

الفصل الخامس
((امن المعلومات وحماية الجهاز))

تاريخ الهكر وبدايتهم

الهاكرز, هذه الكلمة تخيف الكثير من الناس خصوصا مرتادي شبكة الإنترنت الذين يحملون خصوصياتهم الموجودة في أجهزتهم و يبحرون في هذا البحر, و معظم الأحيان يرجعون و قد تلصص أحدهم على هذه الخصوصيات و ربما استخدمها في أمور غير شرعية.

عالم الهاكرز عالم ضخم غامض, و بدايته كانت قبل الإنترنت بل و قبل الكمبيوتر نفسه, و لربما تسائل البعض, من هو الهاكر؟

تعريف الهاكرز:- الهاكرز, هذا اللفظ المظلوم عربيا, يطلق على المتحمسين في عالم الحاسب و لغات البرمجة وأنظمة التشغيل الجديدة, و يستخدم هذا اللفظ ليصف المبرمجين الذين يعملون دون تدريب مسبق.

لقد انتشر هذا المصطلح انتشارا رهيباُ في الآونة الأخيرة و أصبح يشير بصفة أساسية إلى الأفراد الذين يلجئون بطريقة غير شرعية إلى اختراق أنظمة الحاسب بهدف سرقة أو تخريب أو إفساد البيانات الموجودة بها. و في حالة قيام المخترق بتخريب أو حذف أي من البيانات الموجودة يسمى (كراكر), لأن الهاكر يقوم عادة بسرقة ما خف من البرامج و الملفات ولا يقوم بتخريب أو تدمير أجهزة الغير.

بدايتهم :- نعود إلى عام 1878م, في الولايات المتحدة الأمريكية, كان أغلب العاملين في شركات الهاتف المحلية من الشباب المتحمس لمعرفة المزيد عن هذه التقنية الجديدة و التي حولت و غيرت مجرى التاريخ. فقد كانوا يستمعون إلى المكالمات الشخصية و يغيرون الخطوط الهاتفية بغرض التسلية و تعلم المزيد حتى قامت الشركات بتغيير الكوادر العاملة بها من الرجال إلى كوادر نسائية للانتهاء من هذه المشكلة.

مع ظهور الكمبيوتر في الستينات من هذا القرن, انكّب المتحمسون على هذا الصندوق العجيب, و ظهر الهاكرز بشكل ملحوظ, فالهاكر في تلك الفترة هو المبرمج الذكي الذي يقوم بتصميم و تعديل أسرع و أقوى البرامج, و يعتبر كل من (دينيس ريتشي و كين تومسون) أشهر هاكرز على الإطلاق في تلك الفترة لانهم صمموا نظام التشغيل (اليونكس) و الذي كان يعتبر الأسرع في عام 1969م.

و مع ظهور الإنترنت و انتشاره دولياً, أنتجت شركة IBM عام 1981م جهاز أسمته (الكمبيوتر الشخصي) الذي يتميز بصغر حجمه و وزنه الخفيف بالمقارنة مع الكمبيوترات القديمة الضخمة, و أيضا سهولة استخدامه و نقله إلى أي مكان و في أي وقت, و استطاعته الاتصال بالإنترنت في أي وقت.
عندها, بدأ الهاكرز عملهم الحقيقي بتعلم كيفية عمل هذه الأجهزة و كيفية برمجة أنظمة التشغيل فيها و كيفية تخريبها, ففي تلك الفترة ظهرت مجموعة منهم قامت بتخريب بعض أجهزة المؤسسات التجارية الموجودة في تلك الفترة. يوماً بعد يوم ظهرت جماعات كبيرة منافسة , تقوم بتخريب أجهزة الشركات و المؤسسات حتى بدأت هذه المجموعات الحرب فيما بينها في التسعينات من هذا القرن و انتهت بإلقاء القبض عليهم .

و من عمليات الاختراق الملفتة للأنظار, قيام مجموعة من الهاكرز مؤخراً بالهجوم على موقع هيئة الكهرباء والمياه في دبي و مكتبة الشارقة العامة و ذلك بنشر كلمات غريبة في الصفحة الرئيسة للموقعين !

كما قامت مجموعة أخرى من البرازيل باختراق 17 موقعاً من الولايات المتحدة الأمريكية إلى بيرو, و من أهمهم موقع (ناسا) تاركة رسالة تقول " لا نرى فارقاً كبيراً بين نظامكم الأمني و نظام حكومة البرازيل... هل فهمتم؟"

أشهر الهاكرز:- كـــيفن ميتنك, الشخص الذي دوّخ المخابرات الأمريكية المركزية و الفيدرالية FBI كثيراً.

قام بسرقات كبيرة من خلال الإنترنت لم يستطيعوا معرفة الهاكر في أغلبها. و في إحدى اختراقاته، اخترق شبكة الكمبيوترات الخاصة بشركة Digital Equipment Company و سرق بعض البرامج فتم القبض عليه و سجنه لمدة عام.

خرج ميتنك من السجن أكثر ذكاء, فقد كان دائم التغيير في شخصيته كثير المراوغة في الشبكة و كان من الصعب ملاحقته, و من أشهر جرائمه سرقة الأرقام الخاصة ب20000 بطاقة ائتمان و التي كانت آخر جريمة له. و يعتبر ميتنك أول هاكر تقوم الFBI بنشر منشورات عنه تطالب من لديه أية معلومات عته بإعلامها, حتى تم القبض عليه عام 1995 و حكم عليه بالسجن لمدة عام لكنه لم يخرج إلا أواخر عام 1999 و بشرط عدم اقترابه من أي جهاز كمبيوتر لمسافة 100 متر على الأقل!

((ملفات التجسس النصيه))

الموضوع الذي أريد التحدث فيه يختص بأمن نظام التشغيل, أثناء زيارتي لأحد مواقع البحث، قام هذا الموقع بالوصول إلى المتصفح الذي على جهازي (والذي كباقي المتصفحات على الأجهزة العربية مليء بالثغرات)؛ وقام بتغيير الصفحة الرئيسية (Home Page), وباءت كل المحاولات بالفشل لتغيير الصفحة الرئيسية (Home Page).
فقررت أن أقوم بإعادة تنصيب نظام التشغيل. ولكن الأنكى والأمَرّ أنني عدت إلى ذلك الموقع بالخطأ فقررت البحث عن حل جدي للمشكلة .

قُمت بحذف جميع الملفات المؤقتة للانترنت(Temporary Internet Files) وتدمير جميع (Cookies) وبقيت المشكلة على حالها, كل دقيقة يتم تغيير الصفحة الرئيسية (Home Page) ورغم إعادة إقلاع الجهاز مرات كثيرة لم تفلح أياً من الطرق في إيقاف هذه الحالة.

رفعت مستوى الأمان. أزلت الإنترنت إكسبلورر (Internet Explorer). أوقفت سكريبت (Script) بجميع أنواعها ولم تتوقف المشكلة.
بعد عملية بحث على الانترنت اكتشفت الحل :
الذي على جهازي برنامج تجسس كُتب بوساطة الجافا سكريبت (Java Script). و هذا البرنامج يحقن الريجستري (Registry) بالكثير من المفاتيح التي تقوم بتوليد الكود مرة أخرى بعد حذف ملفات الإنترنت المؤقتة (Temporary Internet Files) و لحذف هذا البرنامج نتبع ما يلي:

1- اذهب إلى الموقعhttp://www.lavasoft.de و قم بتحميل البرنامج Ad-aware 6.0 فهو مجاني و لا تنسى أن تقوم بعمل ترقية فلم استطع أن احذف البرنامج حتى قمت بالترقية.
2- قم بتغير إعدادات البرنامج إلى ما يلي:
   1) الصورة



2)   الصورة 2



3-   قم بعد ذلك بتغير أعدادات الأمان (
Security tab) في انترنت إكسبلورر إلى ما يلي :

1)   Download unsigned ActiveX controls – *Disable*

2) Initialize and script ActiveX controls not marked as safe – *Disable*
3) File download – *Disable*
4) Font download – *Disable*
5) Java Permissions – *High safety*
6) Access data sources across domains – Disable
7) Installation of desktop items – *Prompt*
8) Software channel permissions – *High*
9) Allow paste operations via script – *Disable*

4- و من قائمة إعدادات متقدمة (Advanced tab) غير إلى:

1) Check for publisher's certificate revocation.
2) Check for server certificate revocation.
3) Warn about invalid site certificates.
4) Warn if forms submittal is being redirected.

5- بعد ذلك اذهب إلى موقع http://www.zonelabs.com و قم بتحميل ZoneAlarm Pro و ذلك لمنع دخول مثل هذه الملفات على جهازك.

6- بقي أخيراً احتجت لتنصيب Norton AntiVirus 2003 Professional Edition حتى تمكنت من التقاط ملف الجافا سكربيت (Java Script).

كيف اتاكد بان هناك هكر متصل بجهازي

للاتصال بين جهازين لابد من توفر برنامج لكل من الجهازين و يوجد نوعان من البرامج ففي الجهاز

المستهدف (قد يكون جهازك) يوجد برنامج الخادم server و في الجهاز الآخر يوجد برنامج الزبون client و من خلالهما يتم تبادل المعلومات حسب قوة البرنامج الذي بإمكانه الإطلاع على جميع البيانات الموجودة في جهازك و التحكم بنظام التشغيل لديك إلى درجة أن بعضها يمكن أن يفتح سواقة القرص الليزري و يقفلها أو عرض جميع ملفاتك و سحب أو إلغاء أو إضافة.

أما لمعرفة وجود اتصال فالأمر سهل جداً كل ما عليك انه في حاله التأكد من عدم اتصال أي جهاز آخر مع جهازك أن تتجه إلى الدوس و تكتب الأمر الآتي :

C:Windowsnetstat –n

و معناه البحث عن الاتصال بالأرقام عندها سوف تظهر لك شاشه تأخذ ثواني لإعطائك النتيجة و سوف تكون على النحو الآتي :

Proto	Local Address	Foreign Address	State

كل ما يهمنا في الأمر هو الـ Foreign Address و State و سوف تجد في هذا الأمر أرقام مقدم الخدمة لك مع رقم المنفذ port و هنا يجب أن تنتبه لأن الحالة تكون كالآتي:

Foreign Address	State
212.123.234.200:8080	**Established**

أي أن الأرقام 212.123.234.200 هي أرقام مقدم الخدمة ثم تأتي بعدها نقطتين فوق بعض و يأتي بعدها رقم المنفذ و هو 8080 و هذا وضع طبيعي جداً, ثم تأتي كلمة state أي حالة الاتصال و تحتها كلمة Established أي الاتصال تام, و هذا أيضا طبيعي المهم في الأمر إن وجدت رقمIP غريب و تتأكد من ذلك برقم المنفذ و هو الذي يأتي بعد النقطتين التي فوق بعض, مثال :

Foreign Address	State
212.100.97.50:12345	**Established**

انظر إلى رقم الـIP و رقم المنفذ, رقم الـ IP غريب و رقم المنفذ كذلك, إذاً فهو في الغالب منفذ لبرنامج تجسس, و حاله الاتصال تام مع جهازك أي انه بالفعل يوجد شخص الآن داخل

جهازك يتجسس عليك. اكتب رقم المنفذ و هو 12345 ثم اتجه إلى قائمة المنافذ الموجودة في الموقع تحت عنوان أرقام البورتات المستخدمة في برامج التجسس و ابحث عن اسم البرنامج لكي تعرف الملف المصاب به جهازك لتنظيفه

- ثمة طريقة أخرى تختلف قليلا ً عن الأولى. اذهب إلى موجه الدوس و اكتب الأمر التالي:
netstat –a ثم enter و انتظر قليلاً وسوف ترا جميع المنافذ المفتوحة و هي التي تلي الرمز (:) ما قبل الرمز فهو اسم الكمبيوتر الخاص بك الذي تم تعريفه عند تجهيز شبكة الاتصال.
و ضمنها سوف تشاهد الIP الخاص بك و إذا رأيت غير الIP الخاص بك من الممكن ان يدل أن هاكر اخترق جهازك .

المهم قبل ان تكمل يجب ان تغلق جميع المواقع التي تتصفحها لكي لا يعطيكIP المواقع و يخطر على بالك انه هاكرز. المهم ستجد IP واحد هوIP الخاص بك واذا وجدت أكثر منIP احتمال كبير يكون لمخترق, خاصة بعد ان تأكدت انك لا تقوم بتشغيل برنامج محادثة او ليست هناك وسيلة اتصال بين جهازك و بين جهاز اخر على النت, فوجود اتصال آخر غير الذي تعرفه يثير الشك و احتمالية ان يكون لمخترق كبيرة جداً

ماهو الترجوان وكيف اتخلص منه

تعريف:

التروجان هو برنامج تجسس و له أسماء أخرى مثل مخدم (Server) أو اللاصق (Patch) أو الجاسوس (Spy) لكن مبدعين هذا النوع من الملفات يفضلون الأسماء الرنانة و اسم تروجان هو نسبة إلى حصان طروادة. لكن مع اختلاف المسميات فهو برنامج تجسسي يجعل من حاسبك مخدم لحاسب الجاسوس, أي يتمكن الجاسوس (و هو الشخص الذي بعث إليك هذا التروجان) من التحكم بجهازك و كأنه أنت, لكن مع الأخذ بعين الاعتبار أن ذلك فقط في حال أنت متصل بالإنترنت أو الشبكة و ليس هذا فقط بل و عندما يعرف أنك على الإنترنت أما غير ذلك فهو لا حول له ولا قوة.

كيف يلج إلى التروجان إلى حاسبي:

1- عن طريق برامج المحادثة مثل Microsoft chat و ICQ و Mirc و MSN و Yahoo .. الخ.

فلا تستقبل أي ملف مهما يكن و خاصة التي يكون امتدادها exe و حالياً ظهرت برامج تقوم بتغير امتداد الصور إلى exe فبعض الهاكرز يستخدمها في الضحك على الضحايا و يقول لهم أنها صور مغير امتدادها إلى exe و لكنه قد يدس التروجان بداخلها أو قد تكون هي التروجان بحالها.

2- عن طريق البريد الالكتروني:

لذا قم بحذف جميع الرسائل المجهولة و التي لا تعرف من هو مرسلها.

3- عن طريق تحميل برامج من مواقع مشبوهة:

الحل : أن تفعل خاصية الحماية التلقائية لبرنامج Norton Antivirus و الذي هو أقوى برامج الحماية على الإطلاق لأنه يتعامل مع الفيروسات و برامج التجسس على حد سواء.

4- عن طريق المنتديات التي تفعّل خاصية html قد يأتي من هو حاقد على المنتدى و يزرع الكود في رد لموضوع أو في موضوع جديد.

الحل : بسيط جداً لأنه ليس من مسؤوليتك بل من مسؤولية مشرف الموقع.

5- عن طريق الماسنجر بأنواعها هناك برنامج جديد و لكني لا اعلم مدى مصداقية كاتبه و هو يقوم بعمل سرقة الملفات و الصور من جهاز الطرف الآخر إذا كان online و من دون إذنه و اسم البرنامج imesh .

الحل : لا تضيف إلا من تعرفهم و إذا صادفت أي شخص لا تعرفه و شكيت فيه فقم بعمل حظر ثم حذف, لكن إذا كان في جهازك تروجان و حظرته فسوف يدخل و أنت لا تعلم لأن الحظر لن يفيد ما دام الخادم في جهازك يستقبل أوامر العملاء, و أنا لي وقفة بسيطة حول هذا البرنامج قد يكون هذا البرنامج مثل أخواتها من التروجانات .. قد تسمح لمصمم البرنامج أن يتجسس عليك و أنت تحاول أن تتجسس على الآخرين عملاً بشعار افتراس المفترس و هذا هو حال كثير من برامج التجسس.

كيف أتخلص من التروجان إذا أصاب جهازي:

قبل كل شيء يجب أن تعرف أن الملف التجسسي إذا أصاب جهازك فإنه سوف يستوطن في واحد على الأقل من الأماكن التالية:

1- في الريجستري .

2- في الملف Startup .

3- في الملف System.ini .

4- في الملف Win.ini .

أما للتخلص منه فإليك الطريقة..

هناك طريقتين لحذف التروجان و هي مجربة على ويندوز 98 و هي إما بواسطة برامج الحماية و هذه هي الطريقة الأوتوماتيكية, أو الطريقة اليدوية عن طريق DOS و هي الأفضل و الأقوى من خلال التجارب مع Trojans إذا عملت بحث بواسطة برامج الحماية و صدف إنه في بعض الأحيان لا يمكن حذف التروجان بواسطة برامج الحماية لأن التروجان قد يحذف معه ملف مهم من ملفات النظام و في هذه الحالة تضطر إلى استخدام الطريقة الأخرى و هي الأفضل و الأسلم و هي كالتالي:

لنفرض أن التروجان اسمه Server تمكن من معرفته برنامج الحماية, أول خطوة و هي أن تتأكد هل هو يشتغل مع تشغيل الجهاز و ذلك بفعل التالي:

اضغط على زر start

اختر run

اكتب: msconfig

ثم اختر Start UP و من هناك ابحث عن اسم التروجان و غالباً ما يكون اسمه على الاسم الذي تم كشفه, ثم إذا وجدته أزل علامة الصح من أمامه ثم اعد تشغيل الجهاز. يمكنك مراجعة الطرق الاخرى بالضغط على هذه الوصلة

الخطوة الثانية و هي أن تحاول أن تجمع اكبر قدر من المعلومات عن التروجان الذي تم اكتشفاه حتى تتعرف عن أماكن اختبائه في الجهاز و عن تسجيل نفسه في الريجستري أو Win.ini أو System.ini أو جميعها معاً, و أفضل ثلاث مواقع يقدم لك الاستفسار الكامل عن أي تروجان هم

http://www.dark-e.com/archive/trojans/

http://www.google.com/

http://www.moosoft.com/tdbindex.php

الخطوة الثالثة بعد إعادة التشغيل ينبغي أن تكتب اسم التروجان كامل في ورقة خارجية ثم تذهب إلى الدوس عن طريق إعادة التشغيل و اضغط على Ctrl أو F8 أو استخدام قرص الإقلاع اختار Ms-Dos prompt في حال كنت تستخدم Win ME أو عن طريق الدوس الخارجة عن نطاق الويندوز و هي من ابدأ ثم إيقاف التشغيل ثم اختر الرجوع إلى بيئة الدوس RESTART IN MS-DOS MODE و ذلك في حال أنك تستخدم Win 98 ثم اتبع هذه الطريقة لكي تبحث عن التروجان و انتبه إلى المسافة بين الأمر dir و بين اسم التروجان و لا تنسى النجوم *.* :

C:/Windows>dir server *.*

ثم إنتر و إذا وجدت أي ملف اسمه server و امتداده الأخير هو exe فهو مطلبك و عليك أن تحذفه بهذه الطريقة و انتبه إلى المسافة بين deltree و بين اسم التروجان ولا تنسى النجوم *.* :

C:/Windows>Deltree server *.*

ثم إنتر ثم راح تسأل سؤال ضع علامة Y و قد يكون هناك أكثر من برنامج يحمل نفس الاسم و لكن الامتداد يختلف.. أهم شيء انك تبحث عن اسم التروجان server و الذي يكون امتداده exe هذه هي الطريقة اليدوية و الفعالة في حذف التروجان من الجهاز طبعاً تضع بدل من كلمة server الاسم الذي تم رصده من مكافحات التجسس.. ثم اعد تشغيل الجهاز.

ملاحظه مهمة جداً:

هناك أمر أخر للحذف و هو Del و لكني أفضل الأمر Deltree لأنه اشمل في الحذف و يقوم بحذف كل شيء مخفي من اثر التروجان و يتعقبه في كل الأدلة و ليس مثل الأمر Del و الآن نحن في الويندوز و بعدما تم حذف التروجان و بقي أن نزيل بعض من آثاره من win.ini أو system.ini أو الريجستري. طبعاً بعدما تدخل إلى إحدى المواقع اللي فوق و بعدما تبحث عن اسم التروجان الذي تريده أن تعرفه عنه, و كان تروجانك هو server و حصلت على هذه المعلومات من المواقع السابقة و هي انه من فصيلة Sub 7 و أهم شيء من المعلومات هذه من القسم How To Remove و عليك أن تتبع مسار التروجان في مكانه.. و بعد التمحيص عن التروجان وجدناه يسجل نفسه في الريجستري, اذهب إلى المفتاح التالي

HKET_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersion

و ابحث عن الأسماء التالية SERVER.EXEC, EXPLO32, PATCH.EXE, RunDLL32r WINDOWSEXPL32.EXE, , Explorer32, في المفتاحين Run و RunServices و لاحظ على الملفات جيداً فإن لم يقابلها Data أو يظهر أمامها سهم صغير à فهو ملف

تجسس إذ ليس له عنوان معيين في الويندوز, و عندما تجد احد تلك الملفات قم بحذفه, و
بعدين تسوي إعادة تشغيل, و الآن عليك البحث في الملفين Win.ini و System.ini و
اللذين تشغلهما من Run ثم اختر الملف System.ini و ابحث في قسم الـBoot عن أي
اسم غريب تحت هذا السطر shell=Explorer.exe ثم أزل منه الصح لكن تحقق من انه
تروجان و هكذا. بعض التروجانات قد تحذف معها ملفات مهمة من الجهاز و في هذه الحالة
يتطلب منك إرجاعها و طريقة الاسترجاع كالتالي:

في تشغيل Run اكتب SFC ثم إنتر ثم اختر الإعدادات Settings ثم في آخر شيء ضع
علامة صح تفقد الملفات المحذوفة Check for deleted files ثم اختر موافق و بعدها
اختر Start و اترك البرنامج يقوم بعمل فحص للملفات قد يكون هناك ملف محذوف و
يتطلب رجوعه بواسطة CD.. طبعاً على حسب نوع النظام اللي عندك يعني إذا عندك نظام
98 لازم قرص 98 و هكذا إذا وجد ملف محذوف يطلب القرص و أكمل بعدها
إجراءات استرجاعه.

اغلق البوابات الخلفيه

غلق البوابات الخلفية للفيروسات داخل نظام تشغيل ويندوز

نظام تشغيل النوافذ به بعض البوابات الخلفية التي يمكن أن تخترقها الفيروسات من هذه الأبواب تقنية تسمى Windows Scripting Host ويطلق عليها اختصارا WSH فإذا لم تسمع عنها من قبل فيجب أن تقرأ هذا الموضوع بعناية .

الفيروسات الشهيرة مثل فيروس الحب I Love You وفيروس الحب الجديد New Love استغلت هذا الباب لكي تقتحم حاسبات ملاين المستخدمين وتصيبها بأعطال خطيرة .

تقنية WHS تستخدم لكي تسمح لصفحات مواقع الإنترنت بأن تقوم بتشغيل برامج على حاسبات المستخدمين بدون تداخل منهم ومادام قد تم السماح بهذه الخصية فيمكن لصفحات الإنترنت التي تحمل فيروسات أن يتم تشغيلها على الحاسب بنفس الطريقة التي يتم بها تشغيل البرنامج العادي . خاصية WSH اختيارية ويمكن للمستخدم أن يلغيها وبذلك يحمى نفسه من الباب الخلفي لدخول الفيروسات ولكن ليست كل وجود هذا التقنية سيئة فهي لم تخترع لكي تصيب حاسباتنا بالفيروسات ولكن لها فوائد أخرى متعددة ولذلك علينا أن نقارن بين فوائدها وعيوبها وبعد ذلك نقرر هل من الأفضل إلغاؤها أم تركها.

ميزات إلغاء WHS

إلغاء هذه الخصية سيمنع صفحات الإنترنت التي تحمل فيروسات مثل فيروس الحب من العمل . وبذلك لن تتمكن من إلحاق الضرر بحاسبك . وبذلك تصبح ملفاتك في مأمن من الإصابة بهذه الفيروسات الخطيرة . أيضا لن يقوم حاسبك بإرسال نسخة من الفيروسات لحاسبات أصدقائك الذي تراسلهم عن طريق البريد الإلكتروني .

إلغاء هذه التقنية ليس له تأثير سريع ومباشر على حاسباتنا فالحاسب سيستمر في العمل بطريقة طبيعية .

برامج المجموعة المكتبية office وبرنامج الاكسبلور لتصفح الإنترنت لا تستخدم هذه التقنية ولذا فان إلغاء هذه الخصية لا يؤثر على استخدام هذه البرامج.

عيوب إلغاء WHS

بعض البرامج الأخرى غير التي ذكرت قد تستخدم هذه الخصية ولو قمنا بإلغائها فقد يؤثر ذلك على الطريقة التي تعمل بها هذه البرامج وللأسف لا توجد طريقة تخبرنا عن هذه البرامج والتطبيقات التي توجد على الحاسب .ولكن يمكنا القول أن أغلبية البرامج لا تستخدمها .

خطوات إيقاف هذه الخاصية:-

نظام نوافذ 98

- من قائمة البداية اضغط على settings
- اختار التعامل مع لوحة التحكم control panel
- افتح أيقونة Add/remove Programs
- اختار التعامل مع وظيفة windows Setup
- اضغط على مجموعة accessories ثم اضغط على مفتاح details
- الغ العلامة الموضوعة أمام خاصية windows Scripting Host
- اضغط مفتاح ok لتأكيد الاختيار.

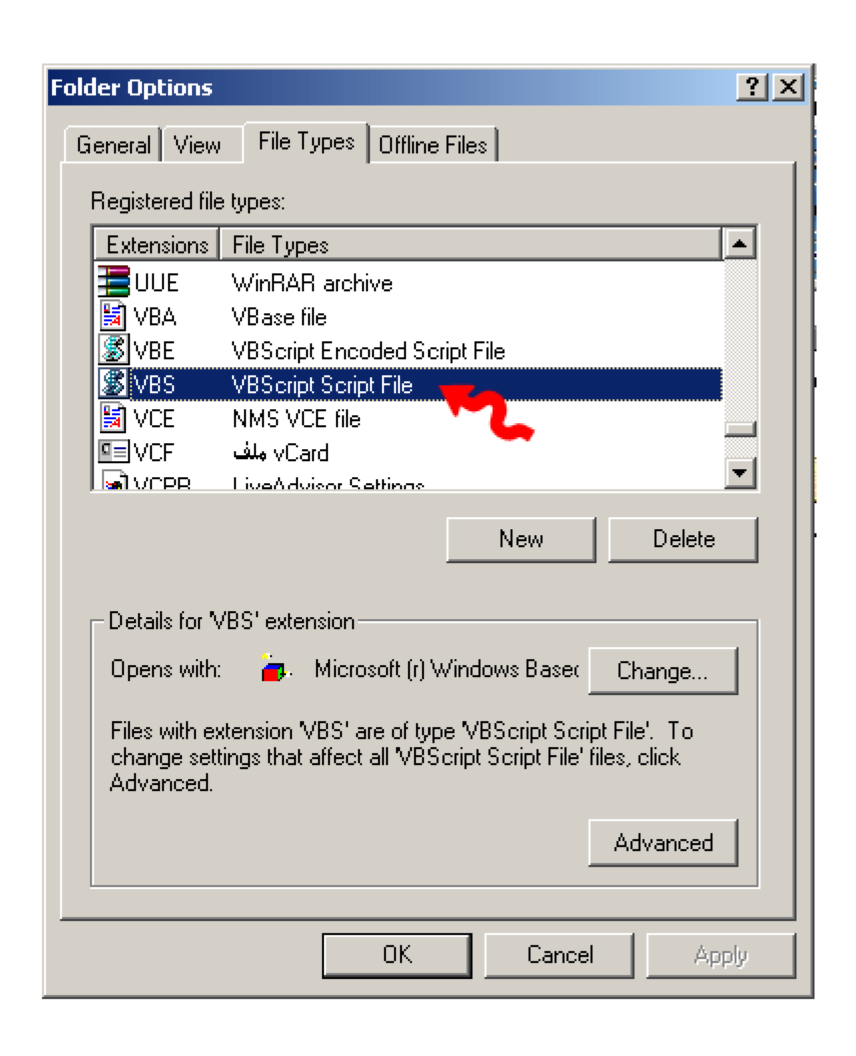
نظام نوافذ 2000

- افتح أيقونة حاسبك myComputer والتي توجد على شاشة سطح المكتب.
- من قائمة الأدوات tools اضغط على اختيارات المجلدات folder Option

- اضغط على وظيفة أنواع الملفات File Types .

- ابحث عن VBScript Script File وقم بإلغائه

- اضغط ok لتأكيد الاختيار.



تعرف على فايروسات الكمبيوتر

لقد سئلنا كثيراً عن الفيروسات و ما هي، و لذا وجدنا من المفيد أن نقدّم لكم بعض المعلومات المفيدة، و كلانا مستعد لأي سؤال أو استفسار ان شاء الله :-)

ماهي الفيروسات؟

فيروسات الكومبيوتر هي برامج تتم كتابتها بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه، تمت كتابتها بطريقة معينة. سُمّيت بالفيروسات، لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين:

- **تحتاج فيروسات الكومبيوتر دائماً إلى ملف عائل تعيش متستّرةً فيه:**
فالفيروسات، دائماً تتستر خلف ملف آخر، و لكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أولاً.
- **تستطيع فيروسات الكومبيوتر أن تنسخ نفسها:**
تتم كتابة هذه البرامج المؤذية بحيث تقوم بنسخ نفسها فوراً بمجرّدتشغيل البرنامج المصاب. و هي تنسخ نفسها للأقراص الأخرى، فإذا كان الكومبيوتر مصاباً ووضعت فيه قرصاً مرناً، يتم نسخ الفيروس اوتوماتيكياً للقرص المرن. و نظراً لهذه الخاصية في الفيروسات، تجد أن القرص المصاب يعطيك علامة أنه ممتلئ تماماً برغم أنك لم تقم بتخزين غير ملفات ذات حجم صغير.

ما الفرق بين الدودة و التروجان و الفيروس؟

- **الدودة:** تصيب الدودة الكمبيوترات الموصلة بالشبكة بشكل اوتوماتيكي و من غير تدخل الانسان و هذا الامر يجعلها تنتشر بشكل اوسع و اسرع عن الفيروسات . الفرق بينهم هو ان الديدان لا تقوم بحذف او تغيير الملفات بل تقوم بتهليك موارد الجهاز و استخدام الذاكرة بشكل فظيع مما يؤدي الى بطء ملحوظ جدا للجهاز , و من المهم تحديث نسخ النظام المستخدم في الجهاز كي يتم تجنب الديدان.

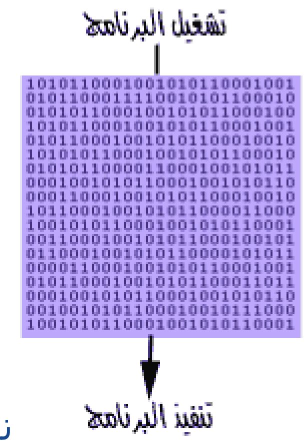
ومن المهم عند الحديث عن الديدان الإشارة إلى تلك التي تنتشر عن طريق الإيميل. حيث يرفق بالرسالة ملفاً يحتوي على دودة، و عندما يشغّل المرسل إليه الملف المرفق، تقوم الدودة بنشر نفسها إلى جميع الإيميلات الموجودة في دفتر عناوين الضحية.

- **التروجان:** وهو عبارة عن برنامج يغري المستخدم باهميته او بشكله او باسمه ان كان جذاباً, و في الواقع هو برنامج يقوم بفتح باب خلفي ان صح التعبير بمجرد تشغيله , و من خلال هذا الباب الخلفي يقوم المخترق باختراق الجهاز و بامكانه التحكم بالجهاز بشكل كبير حتى في بعض الاحيان يستطيع القيام بامور , صاحب الجهاز نفسه لا يستطيع القيام بها , و هذا لا يرجع لملف التروجان, لكن ملف التروجان هو الذي فتح للمخترق الباب ان صح التعبير بتشغيله اياه.

- **الفيروس:** كما ذكرنا , الفيروس عبارة عن برنامج صمم لينشر نفسه بين الملفات و يندمج او يلتصق بالبرامج. عند تشغيل البرنامج المصاب فانه قد يصيب باقي الملفات الموجودة معه في القرص الصلب او المرن, لذا الفيروس يحتاج الى تدخل من جانب المستخدم كي ينتشر , بطبيعة الحال التدخل عبارة عن تشغيله بعد ان تم جلبه من الايميل او تنزيله من الانترنت او من خلال تبادل الاقراص المرنة.

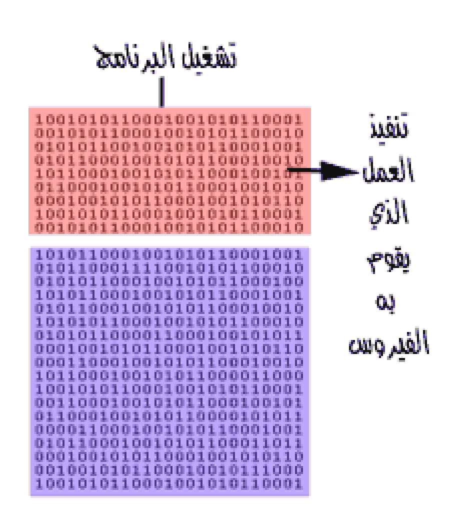
كيف تعمل الفيروسات؟

في الواقع يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهاية الملف المصاب، دون أن يقوم فعلياً بأي تغيير في مكوّنات الملف الأصلية. لننظر للصورة التالية التي توضّح شكل البرنامج غير المصاب بفيروس:

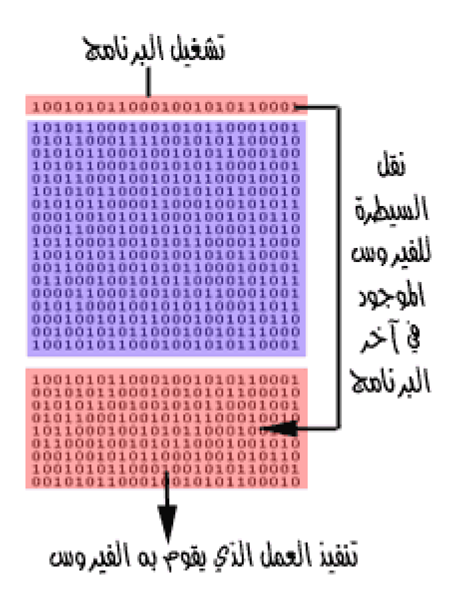


نلاحظ أنه عند استدعاء البرنامج فإنه يعمل بشكل طبيعي.

والآن لنتصوّر أنه تم اصابة البرنامج بفيروس. في الواقع يقوم الفيروس بلصق نفسه في البرنامج كما أسلفنا دون أن يغير في محتويات الملف شيئاً. و طريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه:



وقد تكون طريقة التحاق الفيروس بالملف بأن يضع نفسه في نهاية البرنامج المصاب. و يضع علامة في بدايته، هكذا:



إن هذا الفيروس، يختبئ في نهاية الملف المصاب، و يضع في مقدّمة البرنامج مؤشّراً بحيث أنه عندما يتم استدعاء البرنامج و تشغيله، يحوّل السيطرة للفيروس بدلاً من تشغيل البرنامج.

وفي الحالتين قد يعود الفيروس بعد الانتهاء من تنفيذ عمله المؤذي لتشغيل البرنامج، و لكنه قد لا يعود أيضاً. و يسبب أضراراً جسيمة للجهاز.

أنواع الفيروسات:

هناك الآف من الفيروسات المنتشرة عبر الانترنت , لكن اغلبها ما يقع تحت هذه النقاط الستة:

1. **فيروسات بدء التشغيل او Sector Virus Boot**
هذا النوع من الفيروسات يصيب قطاع الاقلاع في الجهاز , و هو المكان المخصص الذي يتجه اليه الكمبيوتر في بداية تشغيل الجهاز. و هذا النوع من الفيروسات قد يمنع المستخدم من الوصول الى النظام ويمنعه من اقلاع الجهاز.

2. **فيروس الملفات او Virus File**
يصيب البرامج عادة , و ينتشر بين الملفات الاخرى و البرامج الاخرى عند تشغيله.

3. **فيروس الماكرو او Virus Macro**
هذه الفيروسات تصيب برامج الميكروسوفت اوفيس مثل الوورد و الاكسل, و تعتبر ذات انتشار واسع جدا تقدر ب 75% من عدد الفيروسات الموجودة. يقوم هذا النوع من الفيروسات بتغيير بعض المستندات الموجودة في القرص الصلب و خصوصا الوورد , قد تجد بعض التصرفات الغير منطقية في بعض الاحيان مثل طلب باسوورد لفتح ملف تعرف انك لم تضع عليه باسوورد , و ايضا تجد بعض الكلمات قد تغير مكانها و اضيفت كلمات جديدة لا علاقة لها بالموضوع . هي اساساً ليست ضارة, لكنها مزعجة نوعاً ما و قد تكون مدمرة احيانا!

4. **الفيروس المتعدد الاجزاء او Multipartite Virus**
و هو الذي يقوم باصابة الملفات مع قطاع الاقلاع في نفس الوقت و يكون مدمراً في كثير من الاحيان اذا لم تتم الوقاية منه.

5. **الفيروس المتطور او Polymorphic Virus**
هي فيروسات متطورة نوعا ما حيث انها تغير الشفرة كلما انتقلت من جهاز الى آخر. نظريا, يصعب على مضادات الفيروسات التخلص منها لكن عمليا و مع تطور المضادات فالخطر اصبح غير مخيف.

6. **الفيروس المختفي اوVirus Stealth**
تخفي نفسها بان تجعل الملف المصاب سليما و تخدع مضادات الفيروسات بان الملف سليم و ليس مصاباً بفيروس. مع تطور مضادات الفيروسات اصبح من السهل كشف هذا النوع.

ماهي العلامات الشائعة لوجود فيروس في الجهاز:

- بطء الجهاز الشديد، بما لا يتناسب مع عدد البرامج التي تعمل في نفس الوقت.
- امتلاء القرص بما لا يتناسب مع عدد و حجم الملفات الموجودة عليه.
- ظهور مربّعات حوار غريبة اثناء العمل على الجهاز.
- اضاءة لمبة القرص الصلب أو القرص المرن، دون أن تقوم بعملية فتح أو حفظ ملف.

لابد أن تعرف أن هذه العلامات لا تعني بالضرورة وجود فيروس، فقد يكون بعضها بسبب مشكلة في عتاد الجهاز مثلاً.

كيف نحمي أنفسنا من الفيروسات ؟

للحيطة و الحذر من الفيروسات-خاصة إذا كنت معتاداً على تبادل الأقراص المرنة، أو الملفات عبر الانترنت- لابد من اتخاذ الخطوات التالية:

- لابد من موجود برنامج حماية من الفيروسات في جهازك.
- لابد أن تقوم بتحديثه بشكل دوري، وإلا فلا فائدة من وجوده.
- لا تقم بفتح المرفقات في أي إيميل لا تعرف مرسله.
- لا تقم بفتح المرفقات في إيميلات أصدقائك إذا وجدتها تنتهي بـ exe أو bat أو أي امتداد لا تعرفه.
- لا تقبل ملف من شخص لا تعرفه أبداً.
- إذا قبلت ملفاً من شخص تعرفه، افحصه أيضاً ببرنامج الحماية، فقد يكون صديقك نفسه ضحية.
- احرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت، أو تشغيلها من قرص مرن أو سي دي. قبل أن تشغّلها.

داوم على زيارة المواقع التي تهتم بالحماية
من الفيروسات، للإطلاع على كل ما هو جديد في هذا المجال، و لاتخاذ الحيطة، فدرهم
وقاية خيرٌ من قنطار علاج.

معلومات عامة عن برامج الحماية من الفيروسات

كما أسلفنا لابد من وجود برنامج الحماية من الفيروسات في الجهاز. ويقوم البرنامج بفحص و تدقيق الملفات و حماية الجهاز كما ينبغي. وهو يقوم بهذا العمل عن طريق البحث عن بصمات الفيروسات. فلكل فيروس بصمة عبارة عن رقم محدد. و برنامج الحماية في الواقع يبحث عن هذه البصمة المحددة فإن وجدها فإنه يعلن عن وجود الفيروس. وهو اذ يقوم بذلك يقارن بين الملفات و بين جدول
لبصمات الفيروسات المختلفة.

إن الكثير من الفيروسات تتم كتابتها و نشرها في الأسبوع الواحد و هكذا ترى أنه من المهم جداً أن يكون هذا الجدول محدّثاً باستمرار. لذا فإن وجود برنامج الحماية نفسه ليس كافياً أبداً. بل لابد من تحديثه باستمرار.

بعض برامج الحماية من الفيروسات، تقوم بالحماية من التروجانز و الوورمز أيضاً، و لكن هناك بعض البرامج المتخصصة في مجال الحماية من الاختراق، التي تعمل بمساندة برامج المكافحة لحماية جهازك من أي ضرر.

لعل أشهر برامج مكافحة الفيروسات (أو الحماية من الفيروسات) اثنين، هما برنامج Norton للحماية من الفيروسات http://www.norton.com، و برنامج McAffee للحماية من الفيروسات: http://www.mcaffee.com وهذا الموقع يوفّر خدمة الفحص عبر الانترنت مقابل سعر معقول.

و في كلا البرنامجين ستجد رزّا واضحاً في النافذة الرئيسية لتحديث قائمة الفيروسات. فمثلاً في النورتون ستجده في الشكل التالي:



فلا تنسَ القيام بتحديث قائمة الفيروسات بشكل دوري :-)

مواقع مفيدة:

مواقع توفّر معلومات عن الفيروسات:

- موقع يقدّم أحدث المعلومات عن الفيروسات مع ملفات التخلّص منها من مكافي
- تعرّف على الفيروسات و طرق الوقاية منها
- Introduction to viruses
- How Computer Viruses Work

مواقع برامج الحماية من الفيروسات:

- Information Library McAfee's Virus
- AntiVirus Research Center SARC: Symantec
- http://www.antivirus.com

يقدم هذا الموقع إمكانية كشف الفيروسات مجاناً مباشرة عبر النت، و لكن لابد من معرفة أن هذه العملية تعني أنّك تعطي الموقع إمكانية حذف الملفات في جهازك، فإذا شئت فقم بها على مسؤوليتك الخاصة.

ملاحظات مهمّة:

- تتم اصابة جهازك أو قرصك بفيروس فقط حين تقوم بتشغيل برنامج مصاب.
- يمكن لأي قرص أن يصاب بفيروس الـ boot sector.
- مجرّد وجودك في الانترنت لا يعرّضك للاصابة بفيروس. و لكنك تصاب به فقط إذا قمت بتنزيل برنامجاً مصاباً من الانترنت و قمت بتشغيله.
- لابد أن تحرص على استخدام نسخاً قانونية و مسجّلة من البرامج.
- لابد أن تقوم بعمل باك أب لملفاتك المهمة بشكل دوري و ذلك لاسترجاعها في حالة فقدانها لأي سبب تقني أو تعرّضك لفيروس.
- لابد أن يكون في جهازك برنامجاً للحماية من الفيروسات، و لابد أن تقوم بتحديثه بشكل وري.
- لابد أن تقوم بفحص جميع البرامج التي تنوي تشغيلها، و كذلك جميع الأقراص التي تقوم شرائها قبل أن تشغّلها.

نرجو أن يكون الله قد وفّقنا لتغطية جوانب الموضوع المتعددة باختصار و فائدة.

هل تعلم

ان الهكر يمكنه ان يعرف جميع بياناتك
من كلمات السر الخاصه بك

ويستطيع التحكم بجهازك

كفتح سواقة الاقراص
و الكاميرا الخاصه بك
والمايك الخاص بك

ومشاهدة شاشة جهازك

وفتح واغلاق البرامج الخاصه بك
واخذ الملفات التي يريدها
وتنزل ملفات اخرى لجهازك
كلمفات التجسس والفايروسات

كيف يخترق الهكر

عالم الهاكرز عالم دائم التطور, فالهاكرز يخترعون برامج و طرق جديدة معقدة يستطيعون من خلالها اختراق الشبكات و الأجهزة مهما كانت محمية. تختلف برامج التجسس في المميزات و طرق الاستخدام, ولكن الطرق التقليدية التي يستعملها الهاكرز المبتدئين جميعها تعتمد على فكرة واحدة و هي ما يسمى (الملف اللاصق) (Patch file) و الذي يرسله المتجسس إلى جهاز الضحية عن طريق البريد الإلكتروني أو برامج المحادثة فيقوم الأخير بفتحه بحسن نية دون دراية منه أنه قام في نفس الوقت بفتح الباب على مصراعيه للمتجسس ليقوم بما يريد في جهازه, و في بعض الأحيان يستطيع المتجسس عمل ما لا يستطيع الضحية عمله في جهازه نفسه.

يتم الاختراق عن طريق معرفة الثغرات الموجودة في ذلك النظام و غالباً ما تكون تلك الثغرات في المنافذ (Ports) الخاصة بالجهاز, و يمكن وصف هذه المنافذ بأنها بوابات للكمبيوتر على الإنترنت. يستخدم الهاكر برامج تعتمد على نظام (الزبون/الخادم) (client/server) حيث أنها تحتوي على ملفين أحدهما هو الخادم (server) الذي يرسل إلى جهاز الضحية الذي يقوم بفتحه و يصبح عرضةً للاختراق حيث أنه تم فتح إحدى المنافذ بواسطة هذا الخادم.

هناك طرق عديدة و مختلفة تمكن المتطفلين من اختراق الأجهزة مباشرة دون الحاجة إلى إرسال ملفات , لدرجة أن جمعية للها كرز في أمريكا ابتكرت طريقة للاختراق تتم عن طريق حزم البيانات التي تتدفق مع الاتصالات الهاتفية عبر الإنترنت حيث يتم اعتراض تلك البيانات و التحكم في جهاز الضحية. كما يستخدم الهاكرز نظام التشغيل (Unix) لأنه نظام أقوى و أصعب من (Windows) بكثير , كما يستخدمون أجهزة خادمة تعمل على الإنترنت و تستخدم خطوط T1 السريعة الاتصال بالشبكة عن طريق الحصول على حساب شل

((اغلاق المنافذ))

بسبب كثرة السؤال عن طريقة اغلاق البورتات المفتوحه اللي تسهل للهاكرز اختراق الجهاز

نطرح لكم الطريقه وان شاء الله يطبقها الجميع ويغلق بورتاته المفتوحه

وينام قرير العين ويبتعد عن منتهكي الخصوصيه

اتباع الطريقه كما هي :

إذهب إلى :

Start>Runابداء > تشغيل

واكتب الامر التالي

command.com

ستظهر لك نافذة إكتب فيها :

ping host

و إضغط enter ثم إنتظر و اكتب :

ping portو إضغط enter

ثم إنتظر و اكتب :

ping port1027

وإضغط enter

و إنتظر ثم إكتب :

ping port80

و إضغط enter

ثم اكتب :

ping proxy

و إضغط enter

ثم اكتب :

ping port

و إضغط enter

و الآن إنتهت المهمة.. لقد قمت بتقفيل بورت في البروكسي الخاص بك و لقد تم منع دخول الهاكرز من تلك الثغرة الأمنية.

اغلاق البورت 1025

هدا البورت يقوم بفتحه

برنامج هكر اسمه black jack وRemote Storm

المنفذ 1025 هو أول منفذ في المدى الديناميكي لخدمات الآر بي سي (1024 غير مستخدم(
وبالتحديد المنفذ 1025 هو لخدمات Task Scheduler service

ويجب ان يقفل في أسرع وقت devilsmil:...

والطريقه هي

من الدوس اكتب
net stop schedule

ثم

netstat -ano

ثم اكتب الامر التالي ليتم قفله نهائياً
config schedule start= disabled

العلاج والوقايه

كلنا سمع بالحكمة التي تقول (درهم وقاية خير من قنطار علاج) , و طرق الوقاية عديدة تقي الجهاز من الإصابة بفيروسات أو ملفات لاصقة يرسلها هؤلاء الهاكرز, و منها أن يكون الكمبيوتر محملاً ببرنامج (مضاد للفيروسات) و يفضل أن يتم شراؤه لا تنزيله من الإنترنت و يجب تحديثه عن طريق الإنترنت كلما توفر ذلك.من البرامج المضادة للفيروسات برنامج (Norton AntiVirus) الذي يوفر تحديثات كل أسبوعين.

بما أن الغالبية العظمى من الملفات اللاصقة تحتوي على فيروس التروجان (Trojan)- الذي أُخذ اسمه من حصان طروادة صاحب القصة المشهورة, الذي أدخل إلى قصر الطرواديين على أنه هدية من اليونانيين و خرج منه الجنود ليلاً- الذي سيكشفه برنامج المضاد للفيروسات مع باقي الفيروسات إن وجدت, و سيقوم بتنظيف الكمبيوتر من تلك الفيروسات و لكنه لن يتمكن من تنظيف الملفات اللاصقة لأنها تكون قيد العمل بذاكرة الكمبيوتر, هذا إن وُجدت طبعاً.

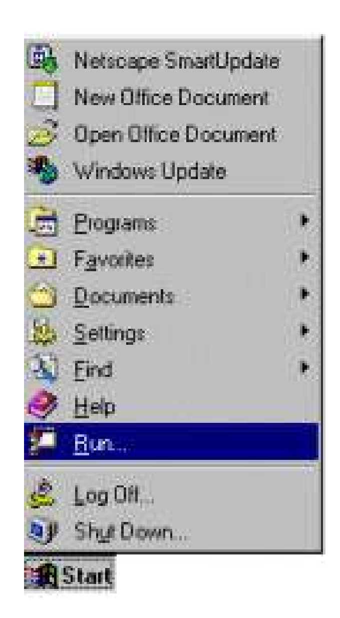
الوقاية:- من الضروري عدم حفظ الملفات الشخصية و الصور العائلية و ملفات تحتوي على أرقام سرية و حسابات في القرص الصلب للجهاز إنما حفظها في أقراص مرنة (Floppy Disk), و الابتعاد عن المواقع المشبوهة عدم تنزيل أي ملفات و برامج منها للاحتمال احتوائها على بعض الفيروسات أو الملفات اللاصقة.

العلاج:- يجب فحص الجهاز بإحدى البرامج المضادة للفيروسات, و عند اكتشافها ملفات تجسس يجب تدوين و تسجيل كل المعلومات عنها على ورقة والاحتفاظ بها.

إن عد الملفات اللاصقة كبير خصوصاً بعد ظهور برامج التجسس الجديدة , لذا قد تكون عملية حذفها صعبة خصوصاً إذا قام الهاكر بتغيير اسم الملف باسم آخر, و لكن سيتم قدر الإمكان تضييق الدائرة على ملف التجسس و حذفه من دفتر التسجيل في الجهاز المصاب و بالتالي منه.

بدخول دفتر التسجيل(Registry) و اتباع التالي:

Start و الضغط على زر run



بكتابة (regedit) في المكان المخصص ستظهر نافذة دفتر التسجيل

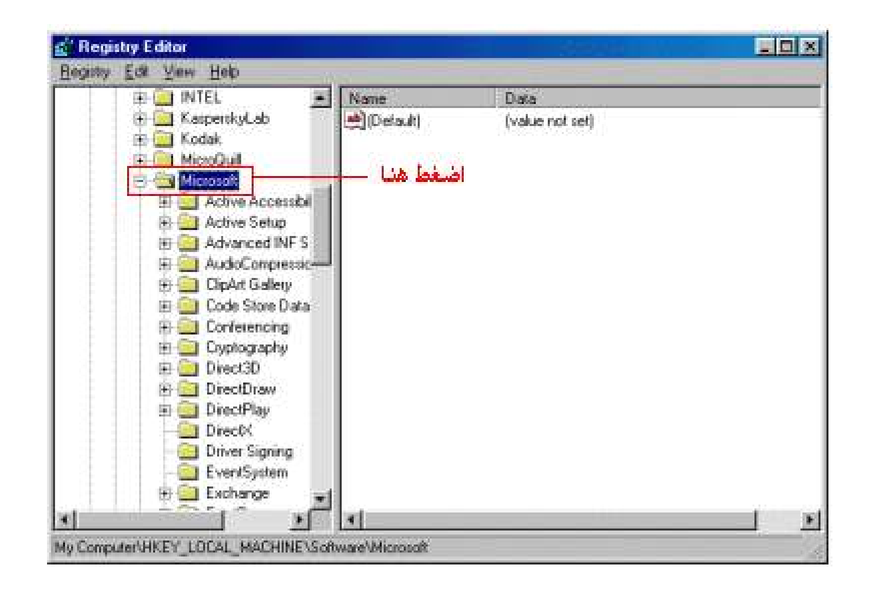


و بالضغط على HKEY-LOCAL-MACHINE

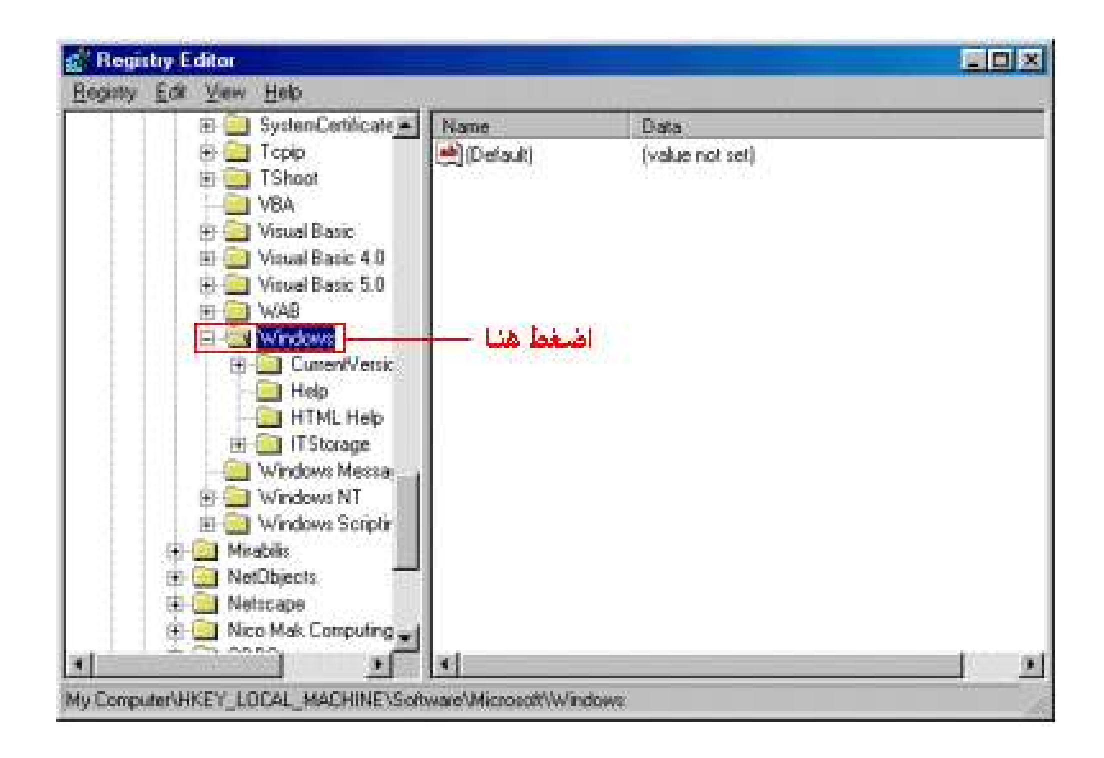
ستظهر قائمة أخرى, و باختيار Software



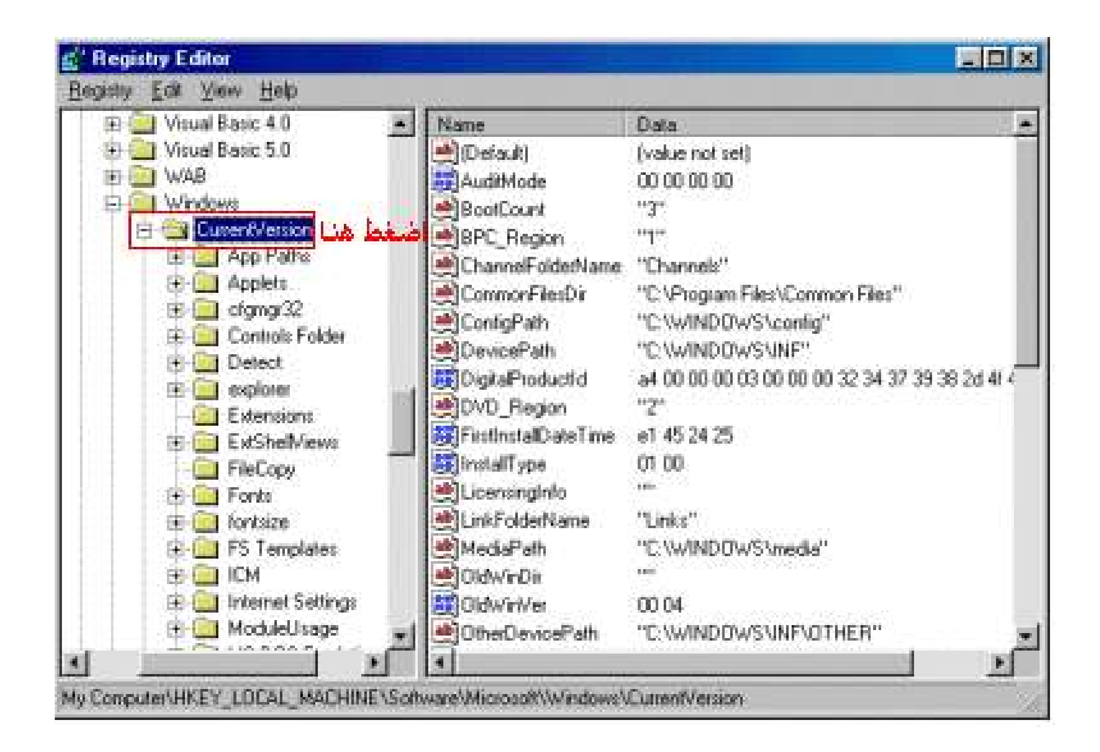
ثم الضغط على زر ال Microsoft ستظهر قائمة أخرى



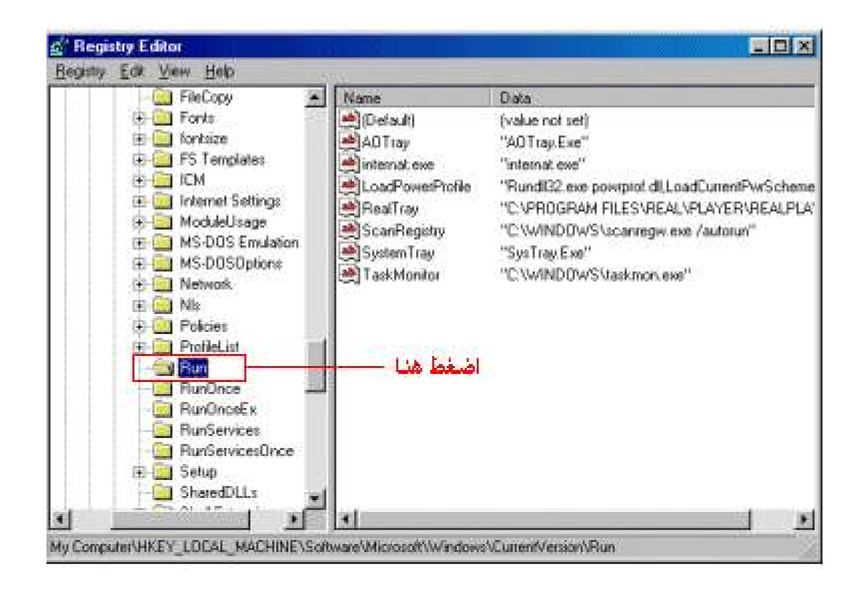
باختيار Windows



ستظهر قائمة أخرى أيضا, بعدها يتم الضغط على Current Version



و أخيراً بالضغط على Run

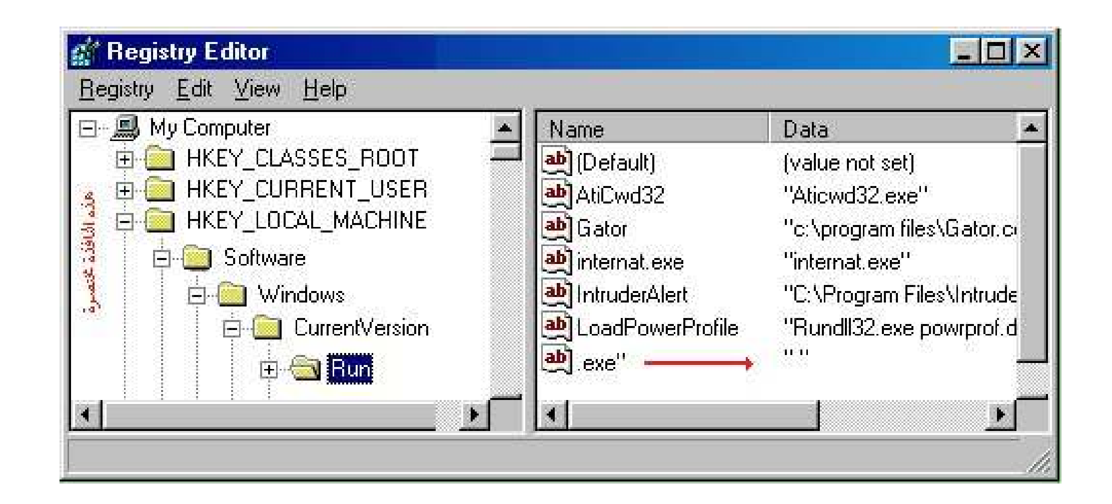


توجد قائمتان

الأولى (Name) و فيها اسم الملفات التي تعمل بقائمة بدء التشغيل للجهاز

الثانية (Data) و فيها معلومات عن الملف و امتداد ه أو البرنامج

من القائمة الثانية نستطيع معرفة ملف التجسس حيث أنه لن تكون له أي معلومات أو امتداد مثل الشكل التالي



فنقوم بحذفه من دفتر التسجيل ثم نقوم بإغلاق النافذة

الخطوة الأخيرة تكون من خلال الذهاب إلى

Start

Restart at MS- Dos

بالذهاب إلى مكان ملف التجسس الذي غالباً ما يكون ملصوقاً بملفات النظام

C:/windows

أو

C:/windows/system متبوعاً باسم الملف , و بحذفه و بإعادة تشغيل الجهاز نكون قد تخلصنا من الملف.

دروس عامه

1-كيف تبحث في GOOgle

يخفى على الكثيرين أهمية مواقع البحث ، فإستخدام الإنترنت مربوط بشكل كبير بهذه
المواقع و طبعاً أضخم هذه المواقع وأشهرها على الإطلاق
هو محرك البحث Google

في هذا الدرس سنذكر بعض الامور المتقدمة في عملية البحث بواسطة محرك البحث google والتعطينا
فهم اوسع عن عملية التحكم بمخرجات و نتائج البحث و التي يمكن استخدام البعض منها مع
محركات البحث الاخرى, لنبدأ على بركة الله:

========================

1- العلامة +

الفائدة منها هي البحث عن جميع المواقع التي تحوي جميع الكلمات .

مثال :

لكي تبحث عن المواقع التي تحوي الكلمتين school و teacher ضع البحث بهذه الصورة : -

school+teacher

========================

2- العلامة -

الفائدة منها هي البحث عن جميع المواقع التي تحوي كلمة و لاتحوي كلمة أخرى

مثال :

لكي تبحث عن المواقع التي تحوي الكلمة school و لا تحوي الكلمة teacher ضع البحث
بهذه الصورة : -

school -teacher

======================

3-علامات التنصيص " "

الفائدة منها هي البحث عن جميع المواقع التي تحوي ما بداخلها بالكامل و بنفس الترتيب

مثال : -

لكي تبحث عن المواقع التي تحوي الجملة please teach me و بالكامل و بنفس الترتيب ضع البحث بهذه الصورة : -

"please teach me"

======================

4- الرابط OR

الفائدة منه هي البحث عن جميع المواقع التي تحوي إحدى الكلمات أو جميعها

مثال : -

لكي تبحث عن المواقع التي تحوي الكلمة school أو الكلمة teacher أو كليهما معاً ضع البحث بهذه الصورة : -

school OR teacher

======================

5) intitle

الفائدة منه هي البحث عن جميع المواقع التي تحوي كلمة في العنوان المخصص للمواقع على google

مثال : -

لكي تبحث عن المواقع التي تحوي الكلمة school في العنوان الظاهر على google ضع البحث بهذه الصورة : -

intitle:school

=======================

allintitle (6

نفس الفائدة من رقم 5 و لكن الفرق أنه هنا بإمكانك أن تبحث عن أكثر من كلمة

مثال : -

لكي تبحث عن المواقع التي تحوي الكلمات school و teacher و book و ذلك في العنوان الظاهر على google ضع البحث بهذه الصورة : -

allintitle:school teacher book

========================

inurl (7

الفائدة منه هي البحث عن جميع المواقع التي تحوي كلمة في عنوان الموقع على الانترنت

مثال : -

لكي تبحث عن المواقع التي تحوي الكلمة school و ذلك في عنوانها على الانترنت ضع البحث بهذه الصورة : -

inurl:school

=========================

allinurl (8

نفس الفائدة من رقم 7 و لكن الفرق أنه هنا بإمكانك أن تبحث عن أكثر من كلمة

مثال : -

لكي تبحث عن المواقع التي تحوي الكلمات school و teacher و book و ذلك في عنوانها على الانترنت ضع البحث بهذه الصورة : -

allinurl:school teacher book

==========================

cache (9

الفائدة منه هي الاستفادة من موقع google لسحب الموقع المراد بالكامل مع الاشارة إلى الكلمات المراد البحث عنها

مثال : -

نريد أن نبحث عن كلمة boy في الموقعWWW.SCHOOL.COM ضع البحث بهذه الصورة : -

cache:WWW.SCHOOL.COM boy

==========================

link (10

الفائدة منه هي إيجاد المواقع التي تحوي رابطاً للموقع المراد البحث عنه

مثال : -

نريد أن نبحث عن المواقع التي تحوي الرابط
WWW.YAHOO.COM ضع البحث بهذه الصورة : -

link:WWW.YAHOO.COM

==========================

related (11

الفائدة منه هي إيجاد الروابط التي يكون فيها الموقع المذكور الصفحة الرئيسية

مثال : -

نريد أن نبحث عن الروابط الموجودة في الموقع WWW.YAHOO.COM ضع البحث بهذه الصورة : -

related:WWW.YAHOO.COM

==========================

info (12

يعطيك معلومات عن الموقع الذي تريده

مثال : -

نريد معلومات عن الموقع WWW.C4ARAB.COM ضع البحث بهذه الصورة : -

info:WWW.C4ARAB.COM

==========================

stocks (13

يستخدم كثيراً مع الرموز لاعطائك معلومات مفصلة مثلاً عليك وضع رمز شركة لا أن تضع اسمها

مثال : -

لكي تحصل على معلومات عن اسعار الاسهم ل Intel و Yahoo
ضع البحث بهذه الصورة : -

stock: intc yhoo

و للبحث بشكل مفصل اكثر يمكنك الضغط على رابط البحث المتقدمة حيث يمكنك التفصيل في عملية البحث في محرك البحث الشهير google.com

2-اظافة خلفيه صوتيه للهوتميل

لإضافة خلفية صوتية في بريد الهوتميل يمكنك ذلك عن طريق استخدام كود بسيط.

الكود هو :

شفرة:

```
<html><BGSOUND balance=0 src="<A
href="http://www.wzeen.com/yas/bgsound.WAV">http://
www.wzeen.com/yas/bgsound.WAV"
volume=0 loop=infinite autostart="true"></html>
```

-

كل ما عليك عمله هو استبدال عنوان الملف الصوتي الموجود في الكود , وذلك بعنوان الملف الصوتي الذي تريد وضعه (عنوان ملف على الإنترنت)

لأدراج الخلفية الصوتية في بريد الهوتميل أتبع التالي :

أذهب إلى بريدك في الهوتميل

في الجزء العلوي من بريد الهوتميل , أختر OPTIONS

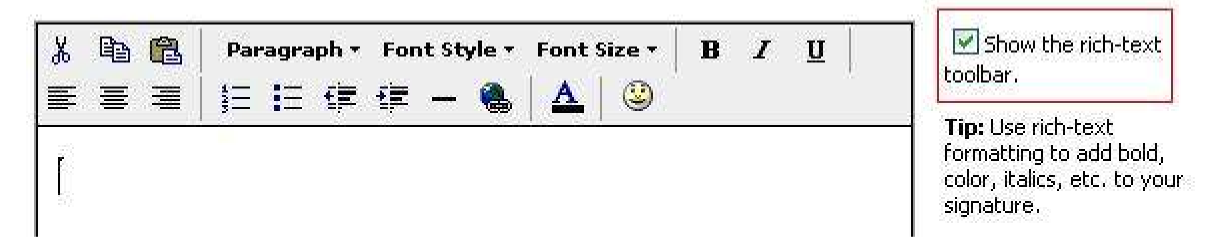


ابحث عن كلمة SIGNATURE وأضغط عليها

ستفتح لك شاشة فيها مربع للكتابة

على يمين المربع موجود ستجد الاختيار Show the rich-text toolbar.

!Error

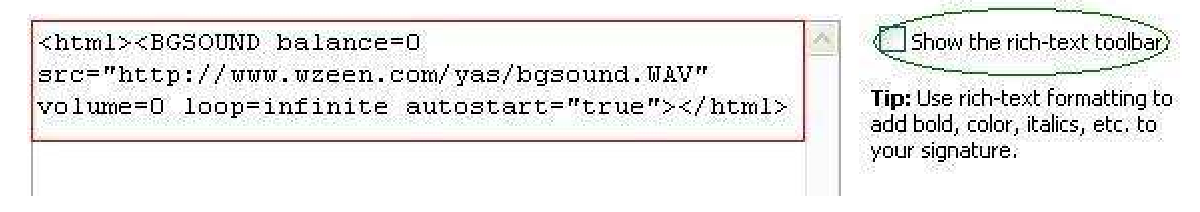


تأكد من إلغاء علامة (صح)

(لابد من إلغاء خاصية RITCH TEXT)

في المربع الذي على الجهة اليسرى , ضع الكود المعدل سابقا

!Error



أضغط على زر OK بالأسفل

وبذلك نكون قد وضعنا خلفية صوتية في توقيعنا في بريد الهوتميل , وعند إرسال أي رسالة سيكون هذا المقطع موجودا بأذن الله

أما إذا أردت وضع المقطع الصوتي في رسالة واحدة فقط ولمرة واحدة فقط أتبع التالي :

أضغط على زر COMPOSE وذلك لكتابة رسالة

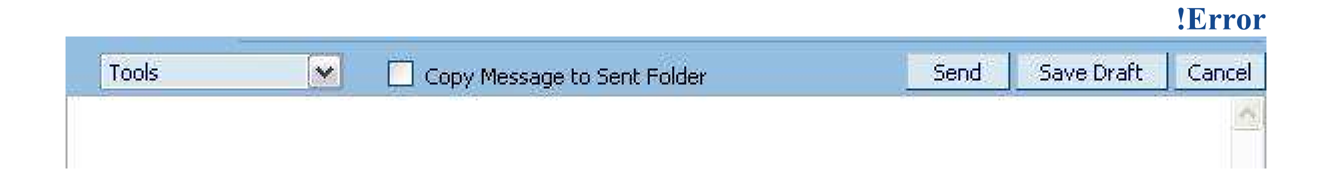
من القائمة المنسدلة للأدواتTOOLS (أسفل مكان كتابة الرسالة)

أختر الاختيار التالي :

OFF RICH-TEST EDITOR

بعد ذلك ضع الكود السابق بعد التعديل في الرسالة وأكتب ما شئت

!Error



ملاحظة هامة :

أرجو من الأخوان عدم استخدام هذه المعلومة فيما حرّم الله , فنحن لسنا بحاجة للمزيد من الآثام

آداب البريد الالكتروني

ان لكتابة البريد الالكتروني آداباً كما لكتابة الرسائل التقليدية آداب ايضاً. سنحاول في هذا الدرس حصر الآداب التي تجعل من الرسالة الالكترونية (الايميل) مرغوبة لدى القارئ و المستقبل لها, ولا يخفى على الكثيرين مدى انزعاج البعض من محتويات و طريقة عرض الرسائل الالكترونية. النقاط التالية تعتبر أهم الامور التي يجب ان تؤخذ في الحسبان و هي ليست مرتبة بحسب الاهمية, و ربما تكون هناك نقاط اخرى لم يتم ذكرها.

1. قصر الرسالة

كثير من الناس يحذف الايميل بمجرد ان يلقى نظرة على طول هذه الرسالة! فاذا كانت رسالة طويلة تحتاج الى تنزيل للصفحة لقراءة بقية محتواها, فان اغلب القرآء لن يقرأوها بكل بساطة, فالكل اصبح مشغولاً و لديه رسائل اخرى لقرائتها! يجب ان تكون الرسالة فيها المطلوب و بالمختصر المفيد , لكي تصل المعلومة الى القارئ باسرع وقت ممكن.

2. اللغة السهلة

ربما يرسل شخص ما رسالة بلهجته المحلية العامية, متناسياً ان المستقبل لها شخص من بلد آخر لا يفهم لهجة المرسل, فلا تتم الاستفادة من ارسال الرسالة و لا توصيل المعلومة. اذا كان المرسل ليس على علاقة مباشرة و شخصية مع المستقبل, فيجب ان يتم ارسال الرسالة بلغة سهلة بسيطة مفهومة و بالعربية الفصيحة لكي يتم التأكد من ايصال المعلومة بدون صعوبات و من اول مرة!

3. عنوان البريد الالكتروني

عنوان البريد الالكتروني هو وسيلة الاتصال بك, بما ان اختيار العنوان الخاص بالبريد الالكتروني هو موضوع اختياري, فان العنوان دائماً ما يشير الي شخصية صاحبه. فعنوان مثل theblankmonkey@somename.com يدل على ان صاحبه يحب القردة السوداء! فان رغب صاحب هذا البريد ان يرسل رسالة الى صاحب شركة مثلاً ليقدم على وظيفة, من الطبيعي ان يلفت نظره عنوان الرسالة و يأخذ فكرة عن صاحبها من غير قراءة السيرة الذاتية حتى!

اذا كان عنوان البريد الالكتروني صعباً, مثل adfd313fss@somename.com , فان الاشخاص الذين يريدون الاتصال بك لن يتمكنوا من هذا الا اذا كان العنوان (مسجل) لديهم , لان ذاكرتهم من الصعب تذكر هذه العناوين عن ظهر قلب!

4

. استخدام الالوان في الرسالة

استخدام الالوان في الرسالة يدل على امور عديدة, شخصية المرسل, حالته عند ارسال الرسالة, الخ من الامور, فحاول اختيار الالوان المناسبة لكل رسالة, اذا كنت ترغب بمراسلة مدير شركة فلا تختر اللون الوردي مثلا!
تجنب اختيار اللون الاصفر الفاقع لانه يؤذي العين و يصعب على القرائ قراءة الكلمات المكتوبة بها.

5. حجم الرسالة

حاول قدر الامكان ان تكون رسالتك صغيرة الحجم, فلا تنسى ان هناك عشرات الرسائل في بريده و اغلب موفري خدمة البريد المجاني يوفرون مساحات قليلة, فلا تجعل مستقبل الرسالة يضطر لحذف رسالة اخرى لسبب رسالتك ذات الحجم الضخم! يمكنك دائماً تحميل الملفات او الصور على موقع مجاني على الانترنت و من ثم وضع رابط التنزيل او الصور في الرسالة, بدل من ارسال الملف او الصور في الرسالة فيصبح حجمها كبيراً.
طبعاً المسألة تختلف من حالة الى اخرى, لكن بشكل عام يجب تصغير حجم الرسالة قدر الامكان.

6. عنوان الرسالة

يجب ان يكون عنوان الرسالة او الايميل واضحاً و قصيراً و يدل على مضمون الرسالة! فاحرص على اختيار العنوان المناسب.

7. الحالة النفسية عند كتابة الرسالة

حاول قدر الامكان ان لا تكتب الرسالة او ترد على رسالة اخرى وانت غاضب او متنرفز, فذلك سينعكس على الرسالة و ستؤدي الى نتائج يمكن ان تتفاداها. احرص على اخذ قسطاً من الراحة و تعوذ بالله من الشيطان, و ابتعد قليلاً عن الجهاز, و ارجع اليه و لكتابة الرسالة بعد ان تهدأ.

8. سرعة الرد

حاول قدر الامكان ان ترد على صاحب الرسالة بأسرع وقت ممكن, خصوصاً للاشخاص الذين ينتظرون منك رداً سريعاً. حاول عدم الاطالة في الرد لان ذلك يزعجهم ولن يعلموا ان كنت قد قرأت الرسالة و تجاهلتها ام قرأتها و لم ترد, او لم تقرأها اصلا.

9. تنسيق الرسالة

اختر خطاً مناسباً لرسالتك, و لا تجعل حجم الخط كبيراً يشعر القارئ بها ان مصيبة قد حصلت! اجعل الرسالة تبدأ من اقصى اليمين ولا تجعلها في المنتصف الا ان كانت نوعية الرسالة تسمح بهذا.

10. القاء التحية

تحية الاسلام هي : **السلام عليكم و رحمة الله وبركاته** , زيّن بها رسالتك و أكسب بها اجر السلام.

قال النبي صلى الله عليه وسلم :والله لا تدخلوا الجنة حتى تؤمنوا ولا تؤمنوا حتى تحابوا أفلا أخبركم بشيء إذا فعلتموه تحاببتم؟ افشوا السلام بينكم.

ابدأ رسالتك بالسلام, و ابدأ ردك برد السلام على مرسل الرسالة, و لا يكفي ان يقول الانسان أهلاً و سهلاً او مرحباً و نحوها من الكلمات.

هذا باختصار, من أهم 10 نقاط حول آداب البريد الالكتروني, ربما تم نسيان بعض النقاط الاخرى و لكن النقاط المذكورة تفي بالغرض ان شاء الله تعالى.


الخاتمه
الإنترنت بحر زاخر, يعج بالجديد الغريب يوميا , و منه
ظهور الهاكرز بهذه الهيئة التطفلية التخريبية, يزداد
عددهم يوميا و تزداد خطورتهم أيضا. لذا وجب أخذ
الحيطة والحذر من هؤلاء المخربين عن طريق حماية
الأجهزة ببرامج مضادة لهم و لطرقهم الجديدة و عن
طريق تحديث هذه البرامج دوريا ليكون الجهاز في
مأمن عنهم, فهم يخترعون كل يوم أشياء جديدة
معقدة , إلى ان تنتهي هذه الحرب ولا اظنها ستنتهي
القرصان2008

الكتاب من تصميم

القرصان و mr.x واميره

Napil_seed@hotmail.com

Hacker.mr.x.@hotmail.com

+966500915561
+966556868205